Juri Ihanus

Tietoturvallisuuden hallintajärjestelmän suunnittelu seurakunnassa

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

11.5.2015

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Juri Ihanus Tietoturvallisuuden hallintajärjestelmän suunnittelu seurakunnassa 48 sivua 11.5.2015
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Talouspäällikkö Iina Vartia Yliopettaja Janne Salonen

Insinöörityössä tutkittiin tietoturvallisuuden hallinnan menetelmiä sekä siihen liittyvää lainsäädännöllistä viitekehystä ja suunniteltiin toimeksiantajalle tietoturvallisuuden hallintajärjestelmän runko. Hallintajärjestelmän avulla tietoon kohdistuvia riskejä voidaan hallita kustannustehokkaasti.

Työn teoriaosuudessa käsiteltiin tietoturvallisuuden peruskäsitteet, osa-alueet sekä sitä ohjaava lainsäädäntö. Teoriaosuudessa painotettiin tietoturvallisuuden hallintaan ja johtamiseen liittyviä asioita. Teoriassa käytettiin enimmäkseen valtiovarainministeriön VAHTI-hankkeen tuottamia ohjeita.

Tietoturvallisuuden hallintajärjestelmällä ja tietoon kohdistuvien riskien hallinnalla on keskeinen rooli tietoturvallisuuden hallinnassa. Hallintajärjestelmä perustuu jatkuvaan kehittämiseen, ja työssä luotu runko mahdollistaa tietoturvallisuuden hallinnan kehittämisen tulevaisuudessa.

Työ tarjoaa kattavan teoriapohjan tietoturvallisuuden hallinnalle ja sitä voidaan käyttää tietoturvallisuuden tason parantamiseen organisaatiossa.

Avainsanat	tietoturva, tietoturvallisuuden hallintajärjestelmä, riskienhallinta, VAHTI

Author(s) Title Number of Pages Date	Juri Ihanus Designing Information Security Management System for Parish 48 pages 11 May 2015
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Information Networks
Instructor(s)	Iina Vartia, Head of Finance Janne Salonen, Principal Lecturer

The thesis studies the theory of information security management, legislation and standards. The aim was to design an information security management system for the Orthodox Parish of Helsinki. The management system enables cost-efficient management of information-related risks.

The theoretical part consists of the basic concepts and aspects of information security and its legislative controls, emphasizing the control and management of information security. The theory focuses on the VAHTI-guidelines authored by Finland's Ministry of Finance.

The information security management system and the management of information-related risks form the core of information security management. The management system bases itself on continuous development, and the framework created in this thesis allows the development of information security management in the future.

The thesis provides a comprehensive theoretical foundation for information security management and it can be used to improve the level of information security in an organization.

Keywords	Information Security, Information Security Management System, Risk Management, VAHTI

Sisällys

Lyhenteet

IP	Internet Protocol, protokolla, joka huolehtii tietoliikennepakettien toimittamisesta pakettikytkentäisessä Internet-verkossa.
ISO	International Organization for Standardization, kansainvälinen standardisoimisjärjestö.
KATAKRI	Kansallinen turvallisuusauditointikriteeristö
VAHTI	Valtionhallinnon tietoturvallisuuden johtoryhmä.

1 Johdanto

Opinnäytetyö on osa projektia, jonka tarkoituksena on kehittää julkisyhteisön tietoturvallisuuden hallintaa ja mahdollistaa tietoturvallisuuden tason ylläpito ja kehittäminen. Työn tavoitteena on tutkia tietoturvallisuuden hallinnan menetelmiä sekä suunnitella keinot tietoturvallisuuden hallinnointiin. Tarkoituksena on kehittää organisaatiolle tietoturvallisuuden hallintajärjestelmän runko, jonka avulla tietoturvallisuuden hallinta mahdollistetaan myös tulevaisuudessa.

Toimeksiantajana toimii Helsingin ortodoksinen seurakunta. Seurakunnan vakituiseen henkilökuntaan kuuluu 60 - 70 työntekijää. Seurakunnan jäsenmäärä on noin 20 000. Seurakunnan tietoturvallisuuden hallinnassa havaittiin puutteita, jolloin aloitettiin projekti tietoturvallisuuden kehittämiseksi.

Monet seurakunnan toiminnot ovat voimakkaasti sidoksissa tietotekniikkaan. Järjestelmissä käsitellään usein tietoa, jonka turvaaminen on tärkeää toiminnan kannalta. Tietoturvallisuuden hallinnointi on tärkeää sekä seurakunnan oman toiminnan että sidosryhmien ja asiakkaiden kannalta.

2 Tietoturvan merkitys

Tietoturvallisuudella tarkoitetaan hallinnollisia, teknisiä ja muita toimenpiteitä, joilla suojataan tietoja, tiedonsiirtoa sekä järjestelmiä, joissa tietoa käsitellään. Toimenpiteillä hallitaan tietoon kohdistuvia riskejä. Tavoitteena on turvata tiedon luottamuksellisuus, eheys ja käytettävyys normaali- ja poikkeusoloissa. Tietoon kohdistuvat riskit voivat olla esimerkiksi järjestelmävikoja, tahallisia tai tahattomia tekoja, luonnontapahtumia tai muita asioita, jotka uhkaavat tiedon eheyttä, luottamuksellisuutta tai käytettävyyttä. [Tietoturvallisuudella tuloksia, VAHTI 3/2007: 13.]

Tietoturvallisuudella on samankaltaisia piirteitä tietosuojan kanssa. Tietosuojan tarkoitus on suojata ihmisen yksityisyyttä ja tiedollista itsemääräämisoikeutta. Tietoturvallisuuden tarjoamilla toimenpiteillä ja menetelmillä on tarkoitus ylläpitää tietosuojaa. Tietoturvallisuutta toteuttaessa on huomioitava tietosuojaa koskevia asioita, joita käsitellään lainsäädännössä. [Laaksonen ym. 2006: 17.]

2.1 Tietoturvallisuuden perusosat

Tietoturvallisuus jaetaan kolmeen perusosaan, joita ovat eheys, luottamuksellisuus ja käytettävyys. Näitä voidaan täydentää pääsynvalvonnalla, kiistämättömyydellä ja tunnistamisella. Tietoturvallisuus perustuu tietoturvallisuuden perusosille asetettujen kriteerien hallintaan. Esimerkiksi täydellisen luottamuksellisuuden saavuttaminen on mahdotonta, mikäli tiedon pitää olla myös käytettävissä.

Eheys tarkoittaa tiedon loogisuutta (sisäinen eheys) ja paikkansapitävyyttä (ulkoinen eheys). Tieto ei saa muuttua hallitsemattomasti onnettomuuksien, vikojen eikä luvattoman tai tahattoman inhimillisen toiminnan seurauksena. Eheyden suojaaminen toteutetaan enimmäkseen teknisiä menetelmiä käyttäen, esimerkiksi virheenkorjausmekanismeja hyödyntäen. Tiedon eheys murtuu esimerkiksi, kun hyökkääjä käyttää tunkeutuu luvatta järjestelmään ja tekee tietoon muutoksia. [Rousku 2014: 49; Tietoturva 2004.]

Luottamuksellisuudella tarkoitetaan sitä, että tietoa voivat käsitellä vain sellaiset tahot, joilla on siihen oikeus. Tiedon luokittelu vaikuttaa siihen, millä tahoilla on oikeus tiedon käsittelyyn. Luottamuksellisuutta parannetaan järjestelmissä esimerkiksi salauksella ja pääsynhallinnalla. Tiedon luottamuksellisuus murtuu esimerkiksi, kun luokiteltu

tieto joutuu luvattoman tahon haltuun. Tiedon vuotaminen luvattomalle taholle voi aiheuttaa suurta vahinkoa tiedon omistajalle. [Rousku 2014: 47-48; Tietoturva 2015.]

Käytettävyydellä tarkoitetaan sitä, että tieto on saatavilla, kun sitä tarvitaan. Tietojärjestelmissä on usein sovittu vasteaika (SLA, service level agreement, palvelutasosopimus), jolloin tiedon on oltava käytettävissä. Nykyään monilta järjestelmiltä edellytetään jatkuvaa käytettävyyttä kellon ympäri. Järjestelmät tarvitsevat kuitenkin välillä huoltokatkoja, eli käytännössä täysin sataprosenttinen palvelutaso on mahdotonta saavuttaa. Tiedon käytettävyys kärsii esimerkiksi palvelunestohyökkäyksistä (DoS, Denial of Service). DoS-hyökkäykset ovat nykyään helppoja toteuttaa, ja jopa isot toimijat ovat kärsineet niistä. [Rousku 2014: 50-51; Tietoturva 2015.]

Tunnistamisella tarkoitetaan kohteen tunnistamista kohteen ominaisuuksien kautta, esimerkiksi työntekijän tunnistamista työympäristöön kuuluvaksi. [Tietoturvan peruskäsitteitä 2012.]

Pääsynvalvonnalla tarkoitetaan sitä, että tietoa pääsee käyttämään vain tunnistettu käyttäjä, jolla on siihen lupa. Pääsynvalvontaan kuuluu todentaminen, tunnistaminen ja valtuutus. Todentamisella viitataan ominaisuuksiin tai tietoon, esimerkiksi salasanat ja kulkukortit kuuluvat todentamisen piiriin. Valtuutuksella tarkoitetaan tunnistetun käyttäjän profilointia, jonka avulla käyttäjälle annetaan käyttöön tietyt oikeudet. Järjestelmissä ei aina käytetä jokaista pääsynvalvonnan osaa. Esimerkiksi kulunvalvontakortin avulla ovessa oleva lukija voi todentaa käyttäjän ja valtuuttaa avaamaan oven. Järjestelmissä ei aina käytetä jokaista pääsynvalvonnan osaa. [Tietoturvan peruskäsitteitä 2012.]

Kiistämättömyydellä tarkoitetaan tiedon keräämistä sen käsittelijöistä siten, ettei kumpikaan osapuoli voi jälkeenpäin kiistää osuuttaan tiedon käsittelyyn. Tämä voidaan toteuttaa esimerkiksi keräämällä talteen tietoa käyttäjistä, jotka ovat viimeksi käsitelleet tiedostoja. [Tietoturvan peruskäsitteitä 2012.]

2.2 Tietosuojan määritelmä

Tietosuojaan kuuluvat yksityiselämän suoja ja muut sitä turvaavat oikeudet henkilötietoja käsitellessä. Tietoturvallisuuden vaarantuessa vaarantuu myös tietosuoja. Henkilötietolaki edellyttää, että tietoja käsitellään hyvän tietojenkäsittelyntavan mukaan. Hyvä

tietojenkäsittelytapa pitää sisällään henkilötietojen ja arkaluonteisten henkilötietojen käsittelyä, laatua ja tietoturvallisuutta koskevat periaatteet. [Asianhallinnan tietoturvallisuutta koskeva ohje, VAHTI 5/2006: 37.]

Hyvän tietojenkäsittelytapa kuuluu hyvään tiedonhallintatapaan, johon kuuluu henkilötietojen suojaaminen, käsittelyn suunnittelu etukäteen, säilytysarvon määrittely sekä henkilötietojen hävittäminen, kun ne käyvät tarpeettomiksi. [Asianhallinnan tietoturvallisuutta koskeva ohje, VAHTI 5/2006: 37.]

2.3 Organisaation tarpeet ja tietoturvallisuus

Nykyaikaisen organisaation tehokkuus, toimivuus ja kehityskyky ovat usein sidoksissa tietojärjestelmiin ja niiden tietoturvallisuuteen. Työntekijät käsittelevät päivittäin tietoa, joka on tärkeää joko organisaatiolle itselleen tai jollekin muulle taholle. Tietoa käsitellään usein tietoteknisillä työkaluilla. Pelkät tekniset ratkaisut eivät kuitenkaan riitä tietoturvallisen ympäristön luomisessa. Tärkeässä roolissa ovat ihmiset, heidän toimintatapansa ja asenteensa. Tietoturvallisuus koskettaakin koko henkilöstöä, eikä pelkästään teknisistä ratkaisuista vastaavia tahoja. [Laaksonen ym. 2006: 19.]

Tietoteknisillä välineillä käsitellään yhä enemmän tietoa, ja uudet teknologiat mahdollistavat tiedon käsittelyn lähes mistä tahansa. Tämä on kasvattanut tietoturvallisuuden vaatimuksia ja yksittäisen ihmisen roolia tietoturvallisuuden osana.

Organisaation tietoturvallisuuden kehittämisen yksi suurimpia haasteita on henkilöresurssien löytäminen tietoturva-asioiden hoitamista varten. Tietoturva-asioiden hoitaminen hyvin on usein edellytys muulle toiminnalle, sillä tietoturvallisuuden romahtaminen voi aiheuttaa ydintoimintojen keskeytymisen. Tietoturvallisuudesta vastaavan tahon pitäisi pystyä keskustelemaan johdon kanssa, että saadaan riittävät resurssit tietoturva-asioiden hoitoon. Tietoturvatoimintojen järkeistäminen ja organisointi lisäävät tehokkuutta, mutta vaativat aluksi paljon resursseja, mikä voi tehdä alusta hankalan. [Laaksonen ym. 2006: 20.]

3 Tietoturvallisuus ja lainsäädäntö

Kansallinen ja kansainvälinen lainsäädäntö velvoittavat organisaatioita tietoturvallisuudesta huolehtimiseen. Lakien määrittelemät velvoitteet ovat usein yleisluontoisia eivätkä ota kantaa käytännön ratkaisuihin tai tietoturvallisuuden tasomäärittelyihin. [Laaksonen ym. 2006: 18.]

Teknisiä tietoturvatoimenpiteitä suorittaessa on usein hankalaa huomioida lain vaatimukset. Lainsäädännön velvoitteet ovat hyvin yleisiä ja tulkittavissa eri tavoin, kun taas tekniset toimenpiteet ovat hyvin tarkkoja. Tekniikan kehittyessä syntyy myös tilanteita, joita lakia säädettäessä ei ole otettu huomioon. [Laaksonen ym. 2006: 18.]

Organisaation tietoturvallisuuden kehityksessä, ylläpidossa ja suunnittelussa tulee ottaa huomioon ohjaava lainsäädäntö sekä organisaation sopimukset, jotka ohjaavat tietoturvallisuutta. [Laaksonen ym. 2006: 18.]

Tässä luvussa käydään läpi tärkeimmät tietoturvallisuuteen liittyvät lait yleisellä tasolla.

3.1 Henkilötietolaki

Henkilötietojen käsittelyssä sovelletaan yleislakina henkilötietolakia (523/1999). Laissa määritellään useita käsitteitä ja vaatimuksia, jotka liittyvät henkilötietojen käsittelyyn. Lain vaatimusten täyttämiseksi on tunnettava lain peruskäsitteet, jotka kiteytyvät hyvään tietojenkäsittelytapaan. Hyvään tietojenkäsittelytapaan kuuluu järjestelmien suunnittelu ja toteutus siten, että yksityisyyden suoja ja rekisteröidyn henkilön oikeudet otetaan huomioon. [Laaksonen ym. 2006: 31-32.]

3.1.1 Henkilölain peruskäsitteet

Henkilötiedolla tarkoitetaan tietoa, joka kuvaa luonnollisen henkilön ominaisuuksia tai elinolosuhteita, joiden avulla voidaan tunnistaa kyseinen henkilö, hänen perheensä tai samassa asunnossa asuvat henkilöt. Henkilötiedoksi voidaan tulkita esimerkiksi nimi, osoite tai muu tieto, jonka perusteella voidaan yksilöidä yksittäinen henkilö. [Laaksonen ym. 2006: 32.]

Henkilörekisterillä tarkoitetaan yhteenkuuluvia henkilötietoja sisältävää tietojoukkoa, jota käsitellään osin tai kokonaan automaattisen tietojenkäsittelyn avulla. Tietojoukko voi olla myös esimerkiksi paperinen järjestetty luettelo, josta tietojen löytäminen onnistuu ilman kohtuuttomia kustannuksia. Yleisiä henkilörekistereitä ovat esimerkiksi organisaation henkilöstöhallinnon rekisteri, joka sisältää työntekijöiden tietoja tai asiakastietoja sisältävä rekisteri. [Laaksonen ym. 2006: 33-35.]

Rekisterinpitäjällä tarkoitetaan yhtä tai useampaa henkilöä tai organisaatiota, jolla on oikeus perustaa henkilörekisteri tai jonka lainmukaisena tehtävänä on rekisterinpito. Rekisterinpitäjän vastuulla on, että henkilötietolakia on noudatettu asianmukaisesti. Organisaation käsitellessä henkilötietoja rekisterinpitäjän vastuu kuuluu organisaatiolle eikä yksittäiselle henkilölle. [Laaksonen ym. 2006: 34.]

Henkilötietojen käsittely tarkoittaa henkilötietoihin kohdistuvia toimenpiteitä, joita ovat henkilötietolain mukaan henkilötietojen kerääminen, tallentaminen, järjestäminen, käyttö, siirtäminen, luovuttaminen, säilyttäminen, muuttaminen, yhdistäminen suojaaminen, poistaminen, tuhoaminen sekä muut toimenpiteet. [Laaksonen ym. 2006: 35.]

Henkilötietolaki vaatii, että henkilötietojen käsittelyn tarkoitus on määritetty. Käytännössä tarkoitetaan sitä, että tiedetään, miksi henkilötietoja kerätään ja mikä taho omistaa kerättävän rekisterin. Kun henkilötietojen käsittelyn tarkoitus on selvä, voidaan ryhtyä suunnittelemaan henkilötietojen käsittelyyn liittyviä prosesseja ja teknisiä toteutuksia. Tässä vaiheessa henkilötietolaki velvoittaa rekisterinpitäjää laatimaan rekisteriselosteen.

Rekisteriselosteesta on selvittävä henkilötietojen käsittelyn tarkoitus, rekisterinpitäjän yhteystiedot, kuvaus rekisteröityjen ryhmästä ja näihin liittyvistä tiedoista, tietojen luovuttamisperiaatteet sekä rekisterin suojausperiaatteet. [Henkilötietolaki (523/1999): 10 §]. Rekisteriselosteessa kuvattavat suojausperiaatteet on syytä pitää riittävän yleisluontoisina, että ei paljasteta liikaa yksityiskohtia tietoturvajärjestelyistä. Kuvauksen yleisluontoisuudella vähennetään myös rekisterin päivitystarvetta. [Laaksonen ym. 2006: 35-36, 39.]

3.1.2 Henkilötietojen käsittelyn periaatteet

Henkilötietojen käsittelyssä on otettava huomioon henkilötietolain määrittelemät periaatteet, jotka ohjaavat rekisterinpitäjän toimintaa ja tietoturvallisuuden suunnittelua. Käsittelyn periaatteet pätevät sekä sähköisesti että manuaalisesti ylläpidettyihin henkilörekistereihin. [Laaksonen ym. 2006: 38.]

Huolellisuusvelvoite tarkoittaa sitä, että rekisterinpitäjän on käsiteltävä henkilötietoja laillisesti, noudattaa huolellisuutta ja hyvää tietojenkäsittelytapaa sekä toimia niin, ettei rekisteröidyn yksityiselämän suojaa ja muita yksityisyyden suojan turvaavia perusoikeuksia rajoiteta ilman laillisia perusteita [Henkilötietolaki (523/1999): 5 §]. Tietojärjestelmien kannalta tämä tarkoittaa sitä, että esimerkiksi käyttöoikeuksien hallinta ja päivityskäytännöt ovat riittävän laadukkaita. Tämä voidaan saavuttaa noudattamalla tunnettuja standardeja ja käytäntöjä. [Laaksonen ym. 2006: 38-39.]

Suunnitteluvelvoite tarkoittaa sitä, että henkilötietojen käsittely on asiallisesti perustelua rekisterinpitäjän toiminnan kannalta. On suunniteltava etukäteen, mistä henkilötiedot hankitaan ja mihin niitä luovutetaan. Henkilötietojen käsittelyn tarkoitus on määriteltävä siten, että on selvää, minkälaisten rekisterinpitäjän tehtävien hoitamiseksi henkilötietoja käsitellään. Suunnitelman tulisi sisältää yleiset periaatteet järjestelmän ja tietoliikenteen turvallisuudesta sekä käyttöoikeuksien myöntämisestä ja käyttöperiaatteista. Suunnittelusta syntyy kirjallinen dokumentti, josta selviää, mitä tietoja prosessissa käsitellään ja miksi niitä käsitellään. Suunnitelman tulisi sisältää myös tietojen käsittelytavat ja vaiheet koko henkilötietojen käsittelyiän ajalta sekä hallinnolliset vastuut henkilörekisterin lupakäytännöistä. [Henkilötietolaki (523/1999): 6 §; Laaksonen ym. 2006: 39.]

Käyttötarkoitussidonnaisuuden tarkoituksena on, että tietoja käsitellään vain käsittelyn suunnittelun mukaisin tavoin [Henkilötietolaki (523/1999): 7 §]. Käytännössä tietoja voidaan siis käyttää vain siihen tarkoitukseen, joka on ennalta määritelty suunnitteluvaiheessa. Jos henkilörekisteri muuttuu siten, että alkuperäinen suunnitelma ei päde, on henkilötietojen käsittely suunniteltava uudelleen. [Laaksonen ym. 2006: 39.]

Virheettömyysvaatimuksella tarkoitetaan sitä, että rekisterinpitäjän vastuulla on huolehtia, ettei virheellisiä, epätäydellisiä tai vanhentuneita tietoja käsitellä [Henkilötietolaki (523/1999): 2, 9 §]. Tietoturvallisuuden kannalta tämä tarkoittaa tietojärjestelmän ehey-

den varmistamista siten, että tieto ei pääse muuttumaan hallitsemattomasti tai auktorisoimattomien tahojen toimesta. [Laaksonen ym. 2006: 40.]

Arkaluonteisiin tietojen käsittely on lain mukaan kielletty, ellei laki sitä erikseen salli. Lain määritelmä arkaluonteisille tiedoille on listattu alla. [Henkilötietolaki (523/1999): 3, 11 §.]

> Arkaluonteisina tietoina pidetään henkilötietoja, jotka kuvaavat tai on tarkoitettu kuvaamaan:
>
> 1) rotua tai etnistä alkuperää;
>
> 2) henkilön yhteiskunnallista, poliittista tai uskonnollista vakaumusta tai ammattiliittoon kuulumista;
>
> 3) rikollista tekoa, rangaistusta tai muuta rikoksen seuraamusta;
>
> 4) henkilön terveydentilaa, sairautta tai vammaisuutta taikka häneen kohdistettuja hoitotoimenpiteitä tai niihin verrattavia toimia;
>
> 5) henkilön seksuaalista suuntautumista tai käyttäytymistä; taikka
>
> 6) henkilön sosiaalihuollon tarvetta tai hänen saamiaan sosiaalihuollon palveluja, tukitoimia ja muita sosiaalihuollon etuuksia.

Arkaluonteisien tietojen voidaan käsitellä lain 12 § mukaisin edellytyksin. Tiedot on poistettava rekisteristä välittömästi kun käsittelylle ei ole enää 12 §:n mukaista perustetta. Tietoja voidaan käsitellä rekisteröidyn erillisellä suostumuksella tai esimerkiksi uskonnollisessa yhteisössä käsiteltävän jäsenrekisterin muodossa.

Henkilötunnuksen käsittely määritellään henkilötietolaissa seuraavasti [Henkilötietolaki 523/1999: 13 §]:

> Henkilötunnusta saa käsitellä rekisteröidyn yksiselitteisesti antamalla suostumuksella tai, jos käsittelystä säädetään laissa. Lisäksi henkilötunnusta saa käsitellä, jos rekisteröidyn yksiselitteinen yksilöiminen on tärkeää:
>
> 1) laissa säädetyn tehtävän suorittamiseksi;
>
> 2) rekisteröidyn tai rekisterinpitäjän oikeuksien ja velvollisuuksien toteuttamiseksi; tai
>
> 3) historiallista tai tieteellistä tutkimusta taikka tilastointia varten.

Henkilötunnusta saa siis käsitellä vain, jos rekisteröidyn yksilöllinen tunnistaminen on tärkeää. Käyttöoikeuksien hallinnassa tulee ottaa huomioon käyttäjän yksilöimisen tarve. Ensisijaisesti yksilöiminen tulisi toteuttaa käyttämällä esimerkiksi tietynmuotoista käyttäjätunnusta henkilötunnuksen sijaan. Lisäksi on huomioitava, että henkilötunnusta ei tulisi merkitä tai siirtää huolimattomasti, esimerkiksi salaamattomalla sähköpostiviestillä. [Laaksonen ym. 2006: 41-42.]

Tietojen suojaamisella tarkoitetaan tarpeellisia teknisiä ja organisatorisia toimenpiteitä henkilötietojen suojaamiseksi asiattomalta pääsyltä ja vahingossa tai laittomasti tapahtuvalta käsittelyltä. Toimenpiteiden toteuttamisessa on huomioitava käytössä olevat tekniset mahdollisuudet, kustannuksen, käsiteltävien tietojen laatu, määrä ja ikä sekä käsittelyn merkitys yksityisyyden kannalta. [Henkilötietolaki (523/1999): 32 §.]

Käytännössä tietojen suojaamisella tarkoitetaan riittävien tietoturvatoimenpiteiden suorittamista luvattoman pääsyn estämiseksi. Tällä tarkoitetaan sekä rekisterin että laitteiston, johon henkilötietoja tallennetaan, suojaamista luvattomalta pääsyltä. Pääsyä ei voida välttämättä estää täysin, koska tekniikalla on rajansa. Mikäli luvaton taho yrittää pääsyä järjestelmään, tulisi yrityksestä aiheutua vähintään hälytys järjestelmän ylläpitäjälle. [Laaksonen ym. 2006: 42.]

Rekisterinpitäjä vastaa riittävän tietoturvatason määrittelystä suojattaville tiedoille. Tason määrittelee ensisijaisesti käsiteltävien tietojen laatu. Esimerkiksi arkaluonteisiksi määritellyt tiedot vaativat korkeampaa tietoturvatasoa kuin esimerkiksi rekisteri, jossa on pelkkiä nimiä. Tietoturvatoimenpiteitä suunnitellessa tulee ottaa tiedon laadun lisäksi huomioon käytettävissä olevat tekniset mahdollisuudet, suojaamisesta johtuvat kustannukset, tietojen määrä ja ikä sekä tietojen käsitellyn merkitys yksityisyyden suojan kannalta. [Laaksonen ym. 2006: 43-44.]

3.1.3 Rangaistussäännökset

Lainvastaisesta henkilötietojen käsittelystä voi seurata vahingonkorvausvelvollisuus. Rekisterinpitäjä velvoitetaan korvaamaan taloudellisen tai muun vahingon rekisteröidylle tai muulle henkilölle lainvastaisesta henkilötietojen käsittelystä. [Henkilötietolaki (523/1999): 47 §.] Henkilötietolain 48 §:ssä säädetään henkilötietolain rangaistussäännökset.

Henkilörekisteririkoksesta ja tietomurrosta aiheutuvat rangaistukset säädetään henkilötietolain 48 §:n mukaan rikoslaissa. Rikoslaki määrittelee tietomurron seuraavasti [Rikoslaki (39/1889): 8 §]:

> Joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja, taikka sellaisen järjestelmän erikseen suojattuun osaan, on tuomittava *tietomurrosta* sakkoon tai vankeuteen enintään yhdeksi vuodeksi.
>
> Tietomurrosta tuomitaan myös se, joka tietojärjestelmään tai sen osaan tunkeutumatta teknisen erikoislaitteen avulla oikeudettomasti ottaa selon 1 momentissa tarkoitetussa tietojärjestelmässä olevasta tiedosta.

Henkilötietolaissa mainitaan myös lainmukaisen vaitiolovelvollisuuden rangaistavuus. Lisäksi rekisterinpitäjä voidaan tuomita sakkoon tai vankeusrangaistukseen lain velvoitteiden noudattamatta jättämisestä. [Laaksonen ym. 2006: 45.]

3.2 Yksityisyyden suoja työelämässä

Lain yksityisyyden suojasta työelämässä (759/2004) tarkoitus on toteuttaa yksityiselämän suojaa turvaavia perusoikeuksia työelämässä. Lain mukaan työntekijällä on oikeus yksityisyyteen ja luottamukselliseen viestintään, vaikka työntekijä käyttäisi työnantajan antamia työvälineitä ja tiloja. [Laki yksityisyyden suojasta työelämässä (759/2004): 1-2 §; Laaksonen ym. 2006: 49.]

Tietojärjestelmät antavat työnantajalle mahdollisuuden kerätä toiminnalle kriittistä informaatiota, mukaan lukien työntekijöiden henkilötietoja. Työntekijällä on intressi hallita tietojen keräämistä ainakin siltä osin, kuin tiedot koskevat häntä itseään. Näin ollen sekä työnantajalle että työntekijälle on tärkeää, että tietojen käsittely tapahtuu tietoturvallisessa ympäristössä ja lainmukaisesti. [Laaksonen ym. 2006: 49.]

Työsopimuslain antaman työnjohto- ja valvontaoikeuden perusteella työnantaja voi antaa työntekijöille työn hoitamiseen liittyviä ohjeita ja määräyksiä. Näihin ohjeisiin tulisi liittää tietoturvaan liittyviä toimenpiteitä, joita työntekijän on noudatettava työpaikalla ja kotona, mikäli käytetään etäyhteyttä. Joidenkin ohjeiden noudattaminen vaatii yhteistoimintamenettelyn, eikä määräystä saa antaa ilman yhteistoimintalain tai -sopimuksen mukaista menettelyä. Käytännössä yhteistoiminta ja tietoturva liittyvät toisiinsa, kun

työpaikalla otetaan käyttöön työntekijöihin kohdistuvaa valvontaa tai kun päätetään tietoverkkojen käyttöön liittyvistä asioista. [Laaksonen ym. 2006: 49-50.]

3.2.1 Tekninen valvonta

Tekniikan kehittyminen mahdollistaa työnantajalle teknisen valvonnan monella eri tavalla. Työnantajan on huomioitava tekniikkaa valittaessa työntekijän yksityisyys ja viestien luottamuksellisuus. Teknisen valvonnan toteutus tulisi dokumentoida ja suunnitella perusteellisesti etukäteen. Dokumentaatiota tulee myös päivittää muutosten yhteydessä. [Laaksonen ym. 2006: 50-51.]

Kulunvalvonnan tarkoitus on estää asiattomien tahojen pääsy tiloihin ja sallia työntekijöiden pääsy työn kannalta tarpeellisiin tiloihin. Kulunvalvonta on lain kannalta kameravalvontaa ”lievempi” valvontakeino. Kulunvalvonta tarjoaa mahdollisuuden paikannustoimintojen käyttämiseen, mutta niiden liittäminen kulunvalvontaan tulisi olla hyvin perusteltua. Perustelu voi olla esimerkiksi työn liikkuva luonne (esim. autonkuljettaja). [Laaksonen ym. 2006: 51-52.]

Kameravalvonta voidaan lähtökohtaisesti järjestää vain lain sallimin edellytyksin. Edellytyksiin kuuluvat työntekijöiden ja muiden tiloissa oleskelevien turvallisuuden varmistaminen, omaisuuden suojaaminen, tuotantoprosessin asianmukaisen toiminnan varmistaminen sekä turvallisuutta, omaisuutta tai tuotantoprosessia vaarantavien tilanteiden ennaltaehkäiseminen tai selvittäminen. Kameravalvontaa ei saa käyttää tietyn työntekijän tai työntekijöiden tarkkailuun työpaikalla. Henkilöstötiloissa, käymälöissä, pukeutumistiloissa tai työntekijän henkilökohtaisessa työhuoneessa ei saa olla kameravalvontaa. Työpisteen kameravalvonta on sallittua vain jos työhön liittyy väkivallan uhka, turvallisuus- tai terveysriskejä, arvokkaan omaisuuden käsittelyä tai mikäli valvonnalla voidaan varmistaa työntekijän etuja ja oikeuksia ja asiasta on sovittu työntekijän ja työnantajan välillä. [Laki yksityisyyden suojasta työelämässä (759/2004): 16 §.]

Lähtökohtaisesti kameravalvonnasta syntyviä tallenteita tulee käyttää vain tarkkailun suunnitellun tarkoituksen täyttämiseksi. Tallenteita voidaan käyttää poikkeuksellisesti suunnitellun tarkoituksen lisäksi työsuhteen päättämisen perusteen todennäyttämiseksi, esimerkiksi tietoturvaan liittyvien vakavien väärinkäytösten ja epäasiallisen käytöksen selvittämiseksi, jos työnantajalla on perusteltu aihe epäillä työntekijää epäasiallisesta käytöksestä, laiminlyönneistä tai vastaavasta ei-sallitusta käytöksestä. Esimer-

kiksi toisen työntekijän pahoinpitely voi olla peruste tallenteiden käyttämiseen poikkeuksellisesti. Tallenteet on hävitettävä, kun ne eivät ole enää tarpeellisia valvonnan tarkoituksen toteuttamiseksi ja viimeistään vuoden päästä tallentamisen päätyttyä. Edellä mainittujen poikkeustilanteiden selvittämisessä käytettäviä tallenteita voidaan kuitenkin poikkeuksellisesti säilyttää, kunnes selvittely on saatettu loppuun. Laissa mainitaan myös muut erityiset syyt, joita voi olla esimerkiksi työnantajalle kuuluvat velvoitteet tai erilaiset turvallisuusnormit. [Laki yksityisyyden suojasta työelämässä (759/2004): 17 §; Laaksonen ym. 2006: 52-54.]

3.2.2 Rangaistussäännökset

Lain 24 §:n mukaan työnantaja tai tämän edustaja, joka tahallaan tai törkeästä huolimattomuudesta rikkoo lain suojaamia oikeuksia, voidaan tuomita sakkoon, jollei muualla laissa säädetä ankarampaa rangaistusta. Rangaistus henkilörekisteririkoksesta, tietomurrosta, salakatselusta, salakuuntelusta, viestintäsalaisuuden loukkauksesta, salassapitorikoksesta ja virkarikoksista säädetään rikoslaissa. [Laki yksityisyyden suojasta työelämässä (759/2004): 24 §; Laaksonen ym. 2006: 54.]

3.3 Tietoyhteiskuntakaari

Tietoyhteiskuntakaari (917/2014) korvasi vuoden 2015 alusta useita vanhempia säädöksiä, mukaan lukien sähköisen viestinnän tietosuojalain (516/2014), viestintämarkkinalain (393/2003) ja verkkotunnuslain (228/2003).

Lain 1 § määrittää lain tavoitteet seuraavasti [Tietoyhteiskuntakaari (917/2014): 1 §]:

> Lain tavoitteena on edistää sähköisen viestinnän palvelujen tarjontaa ja käyttöä sekä varmistaa, että viestintäverkkoja ja viestintäpalveluja on kohtuullisin ehdoin jokaisen saatavilla koko maassa. Lain tavoitteena on lisäksi turvata radiotaajuuksien tehokas ja häiriötön käyttö sekä edistää kilpailua ja varmistaa, että viestintäverkot ja -palvelut ovat teknisesti kehittyneitä, laadultaan hyviä, toimintavarmoja ja turvallisia sekä hinnaltaan edullisia. Lain tavoitteena on myös turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen.

Lain valmistelun pääteemoina olivat yksityisyyden ja kuluttajansuojaa koskevien säännösten tarkistaminen, säännösten vähentäminen, selkeyttäminen sekä päällekkäisten säännösten poistaminen, toimilupajärjestelmän uudistaminen, toiminnan harjoittajan

velvoitteet sekä sähköisen viestinnän ja palveluiden turvaaminen. [Tietoyhteiskuntakaari 2015.]

3.3.1 Tietoyhteiskuntakaaren peruskäsitteet

Laissa on useita käsitteitä, joiden ymmärtäminen auttaa hahmottamaan lain sovellusta. Tässä keskitytään työn toimeksiantajan kannalta keskeisimpiin käsitteisiin.

Lain 3 § määrittelee kyseiset käsitteet seuraavasti [Tietoyhteiskuntakaari (917/2014): 3 §]:

> 7) *käyttäjällä* luonnollista henkilöä, joka palvelun tilaajana tai muuten käyttää viestintäpalvelua tai lisäarvopalvelua;
>
> 10) *lisäarvopalvelulla* palvelua, joka perustuu välitystietojen tai sijaintitietojen käsittelyyn muuta tarkoitusta kuin viestin välittämistä varten;
>
> 18) *sijaintitiedolla* viestintäverkosta tai päätelaitteesta saatavaa tietoa, joka ilmaisee liittymän tai päätelaitteen maantieteellisen sijainnin ja jota käytetään muuhun kuin viestin välittämiseen;
>
> 22) *sähköisellä viestillä* tietoa, jota välitetään tai jaetaan sähköisesti;
>
> 28) *tietoturvalla* hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, että tietoja eivät voi muuttaa muut kuin siihen oikeutetut sekä että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä;
>
> 36) *viestinnän välittäjällä* teleyritystä, yhteisötilaajaa ja sellaista muuta tahoa, joka välittää sähköistä viestintää muutoin kuin henkilökohtaisiin tai niihin verrattaviin tavanomaisiin yksityisiin tarkoituksiin;
>
> 39) *viestintäverkolla* toisiinsa liitetyistä johtimista sekä laitteista muodostuvaa järjestelmää, joka on tarkoitettu viestien siirtoon tai jakeluun johtimella, radioaalloilla, optisesti tai muulla sähkömagneettisella tavalla;
>
> 40) *välitystiedolla* oikeus- tai luonnolliseen henkilöön yhdistettävissä olevaa tietoa, jota käsitellään viestin välittämiseksi sekä tietoa radioaseman tunnisteesta, radiolähettimen lajista tai käyttäjästä ja tietoa radiolähetyksen alkamisajankohdasta, kestosta tai lähetyspaikasta;
>
> 41) *yhteisötilaajalla* viestintäpalvelun tai lisäarvopalvelun tilaajana olevaa yritystä ja yhteisöä, joka käsittelee viestintäverkossaan käyttäjien viestejä, välitystietoja tai sijaintitietoja;

Määritelmät ovat muuttuneet aikaisemmasta lainsäädännöstä vain vähän. Esimerkiksi aikaisemmin sähköisen viestinnän tietosuojalaissa käytetty määritelmä *tunnistamistieto* ei ole enää käytössä, vaan se on korvattu *välitystiedolla.*

3.3.2 Tunnistamistietojen käsittely

Viestin ja välitystietojen luottamuksellisuudella rajoitetaan sähköisten viestien käsittelyoikeuksia. Lain mukaan viestinnän osapuolilla on lähtökohtaisesti oikeus käsitellä viestejään ja niiden välitystietoja. Myös lain määrittelemää yleistä radioviestintää ja sen välitystietoja saa käsitellä. Muiden viestin ja välitystietojen käsittely vaatii lähtökohtaisesti viestinnän osapuolen suostumuksen. Jos saa haltuunsa viestin, tai tiedon viestistä, eikä kuulu niihin, joilla on oikeus käsitellä viestiä, ei saa ilman viestinnän osapuolien suostumusta ilmaista tai käyttää hyväksi viestin sisältöä tai välitystietoa tai tietoa viestin olemassaolosta. [Tietoyhteiskuntakaari (917/2014): 136 §.]

Viestinnän välittäjän yleisiin käsittelyperiaatteisiin kuuluu, että käsittely on sallittua ainoastaan käsittelyn tarkoituksen vaatimassa laajuudessa, eikä sillä saa rajoittaa luottamuksellisen viestin ja yksityisyyden suojaa enempää kuin on välttämätöntä. Viestejä ja välitystietoja saa luovuttaa vain niille, joilla on oikeus käsitellä tietoja asianomaisessa tilanteessa ja käsittelyn jälkeen ne on hävitettävä tai tehtävä sellaisiksi, ettei niitä voi yhdistää tilaajaan tai käyttäjään. Käsittelyn hoitaa joko viestinnän välittäjä tai tilaajan lukuun toimiva taho. [Tietoyhteiskuntakaari (917/2014): 137 §.]

Viestien käsittelyperusteet määritellään lain 17 luvussa. Viestin välittäjä voi käsitellä viestejä ja välitystietoja vain määriteltyjen tarkoitusten puitteissa.

Lain 17 luku sisältää seuraavat käsittelyperusteet [Tietoyhteiskuntakaari (917/2014): 137 §-144 §]:

- viestinnän välittäminen, palvelun toteuttaminen ja tietoturvasta huolehtiminen
- laskutus
- markkinointi
- tekninen kehittäminen
- tilastollinen analyysi

- väärinkäytöstapausten havaitseminen, estäminen tai selvittäminen
- teknisen vian tai virheen havaitseminen, estäminen tai selvittäminen.

Viestinnän välittäjän tulee tallentaa yksityiskohtaiset tapahtumatiedot tapahtuneesta välitystietojen käsittelystä, jos se on mahdollista teknisesti ja ilman kohtuuttomia kustannuksia. Tapahtumatiedot on säilytettävä kaksi vuotta, ja niistä on käytävä ilmi käsittelyn ajankohta, kesto ja käsittelijä. Lain mukaan Viestintävirasto voi antaa tähän vaatimukseen liittyen tarkempia määräyksiä. [Tietoyhteiskuntakaari (917/2014): 145 §.]

Yhteisötilaajaa koskeva erityissääntely tarkentaa yhteisötilaajien oikeuksia ja velvoitteita. Yhteisötilaajalla on oikeus käsitellä viestejä ja välitystietoja luvattoman käytön tai yrityssalaisuuksien paljastamisen ehkäisemiseksi lain määräämin keinoin ja velvoittein. Luvattomaksi käytöksi katsotaan yhteisötilaajan verkkoon laitteen, ohjelman tai palvelun asentaminen, oikeudettoman pääsyn avaaminen tai muu vastaava yhteisötilaajan määrittelemän verkon käyttötarkoituksen vastainen toiminta. Käsittelyoikeus ei koske puhelinpalvelujen välitystietoja. [Tietoyhteiskuntakaari (917/2014): 146 §.]

Yhteisötilaajan huolehtimisvelvollisuudella tarkoitetaan toimia, jotka yhteisötilaajan on hoidettava ennen välitystietojen käsittelyä. Ennen välitystietojen käsittelyä luvattoman käytön ehkäisemiseksi, yhteisötilaajan on rajoitettava pääsyä verkkoonsa ja suojattava sen käyttö asianmukaisin tietoturvallisuustoimenpitein sekä määriteltävä minkälaisia viestejä verkossa saa siirtää ja mihin viestintää voidaan harjoittaa. [Tietoyhteiskuntakaari (917/2014): 147 §.]

Yhteisötilaajan suunnittelu- ja yhteistoimintavelvoitteen mukaan ennen välitystietojen käsittelyn aloittamista yhteisötilaajan on nimettävä henkilöt tai tehtävät, joille välitystietojen käsittely kuuluu. Lain mukaan vain yhteisötilaajan viestintäverkon ylläpidosta ja tietoturvasta sekä turvallisuudesta huolehtivat henkilöt voivat käsitellä välitystietoja. Yhteistoimintalain piiriin kuuluvat työnantajan on käsiteltävä välitystietojen käsittelyn perusteet ja käytännöt yhteistoimintalain mukaisin menettelyin ja tiedotettava päätöksensä työntekijöille yksityisyyden suojasta työelämässä annetun lain mukaisesti. Mikäli yhteisötilaaja ei työnantajana kuulu yhteistoimintalain piiriin, on hänen kuultava työntekijöitä välitystietojen käsittelyssä noudatettavista menettelyjen perusteista ja käytännöistä sekä tiedotettava niistä kuten yksityisyyden suojasta työelämässä annetussa laissa säädetään. [Tietoyhteiskuntakaari (917/2014): 148 §.]

Yhteisötilaajan käsittelyoikeudet määrittävät laissa, millä keinoin yhteisötilaaja saa käsitellä välitystietoja. Lähtökohtaisesti välitystietojen käsittely on suoritettava automaattisen haun avulla, esimerkiksi viestin koon, tyypin, määrän tai kohdeosoitteen perusteella. Manuaalinen käsittely sallitaan, jos on syytä etukäteen epäillä, että käsiteltävää viestintäverkkoa, viestintäpalvelua tai maksullista tietoyhteiskunnan palvelua käytetään yhteisötilaajan määrittämien tarkoitusten vastaisesti. [Tietoyhteiskuntakaari (917/2014): 149 §.]

Manuaalisen käsittelyn muihin perusteisiin kuuluvat [Tietoyhteiskuntakaari (917/2014): 149 §]:

> 1) automaattisen hakutoiminnon avulla on havaittu viestinnässä poikkeama;
>
> 2) maksullisen tietoyhteiskunnan palvelun käytön kustannukset ovat nousseet epätavallisen korkeiksi;
>
> 3) viestintäverkossa havaitaan sinne oikeudetta asennettu laite, ohjelma tai palvelu; taikka
>
> 4) yksittäistapauksessa muusta 1–3 kohtaan rinnastuvasta, yleisesti havaittavissa olevasta seikasta voidaan päätellä, että viestintäverkkoa, viestintäpalvelua tai maksullista tietoyhteiskunnan palvelua käytetään 147 §:n 3 momentissa tarkoitettujen ohjeiden vastaisesti.
>
> Edellä 1 ja 2 momentissa tarkoitetun käsittelyn edellytyksenä on, että tapahtuma tai teko todennäköisesti aiheuttaa yhteisötilaajalle merkittävää haittaa tai vahinkoa.
>
> Edellä 2 momentissa tarkoitetun käsittelyn edellytyksenä on lisäksi, että tiedot ovat välttämättömiä luvattoman käytön ja siitä vastuussa olevien selvittämiseksi sekä luvattoman käytön lopettamiseksi.

Yhteisötilaajan on lisäksi tehtävä selvitys työntekijöiden edustajalle vuosittain manuaalisesta käsittelystä, josta on käytävä ilmi, millä perusteella ja montako kertaa välitystietoja on käsitelty vuoden aikana. Tietosuojavaltuutetulle on myös tehtävä vuosittainen selvitys ja ilmoitus välitystietojen käsittelyn aloittamisesta. Laissa säädetään myös yhteisötilaajan oikeuksista luovuttaa ja säilyttää välitystietoja väärinkäytöstapauksissa. [Tietoyhteiskuntakaari (917/2014): 152-156 §.]

3.3.3 Yhteisötilaajan tietoturvatoimenpiteet

Tietoyhteiskuntakaaressa säädetään tietoturvan toteuttamiseksi ja poikkeamatilanteiden hallitsemiseksi tehtävistä toimenpiteistä viestintäverkoissa ja viestintäpalveluissa. Viestintävirasto voi lain mukaan antaa tarkempia määräyksiä toimenpiteiden suorittamisesta.

Teleyrityksellä, yhteisötilaajalla ja lisäarvopalvelun tarjoajalla on oikeus selvittää automaattisesti viestien sisältöjä, rajoittaa viestien välittämistä ja vastaanottoa, poistaa automaattisesti haitallista sisältöä viesteistä sekä suorittaa muita vastaavia teknisiä toimenpiteitä. Edellä mainitut asiat sallitaan, kun tutkitaan viestintäverkon tai siihen liitetyn järjestelmän tai palvelun häiriöitä, kun turvataan viestinnän osapuolien viestintämahdollisuuksia tai kun toteutetaan rikoslain mukaisesti maksuvälinepetosten valmistelun ehkäisemistä. Jos automaattinen käsittely ei havaitse haitallista ohjelmaa tai vastaavaa, voidaan käsittely suorittaa manuaalisesti, jos on ilmeistä, että viesti sisältää haitan. [Tietoyhteiskuntakaari (917/2014): 272 §.]

Verkkolaitteen tai viestintäverkon tai sen sisältämän palvelun aiheuttaessa merkittävää häiriötä toiselle viestintäverkolle, palvelulle tai henkilölle, on verkon haltijan korjattava virhe ja tarvittaessa poistettava häiriön lähde yleisestä viestintäverkosta. Toimenpiteissä on otettava huomioon häiriön vakavuus, eikä toimenpiteillä saa rajoittaa sananvapautta tai lain säätämää luottamuksellisen viestin suojaa tai yksityisyyden suojaa. Rajoittavat toimenpiteet on lopetettava, jos häiriö saadaan poistettua. [Tietoyhteiskuntakaari (917/2014): 273 §.]

3.4 Laki viranomaisen toiminnan julkisuudesta

Laki viranomaisen toiminnan julkisuudesta (julkisuuslaki) säätelee viranomaistoiminnan asiakirjan- ja tiedonhallintaa. Lain lähtökohtainen tarkoitus on viranomaistoiminnan ohjaaminen, mutta sillä on yhtymäkohtia henkilötietolakiin. Lain sisältöön kuuluu erityissuojattavan tietoaineiston luokittelu, luovutusperiaatteet ja salassapitovelvoitteet. [Laaksonen ym. 2006: 29-30.]

Julkisuusperiaatteen mukaan kaikki viranomaisen asiakirjat ovat lähtökohtaisesti julkisia, ellei salassapidosta säädetä muutoin laissa [Laki viranomaisten toiminnan julki-

suudesta (1999/621): 1 §]. Asiakirjojen salassapito on siis julkisuusperiaatteen poikkeustapaus. [Laaksonen ym. 2006: 29.]

Suojattavat tietoaineistot luokitellaan lain mukaisesti kolmeen luokkaan: erittäin salaiset, salaiset ja luottamukselliset tietoaineistot. Luokittelu perustuu tiedon oikeudettomasta paljastumisesta tai käytöstä seuraavaan haittaan. Laki ei määrittele tarkemmin, mitä vaatimuksia luokittelutasot asettavat tietoturvallisuudelle. Julkishallinnolle on kuitenkin olemassa suuri määrä valtiovarainministeriön VAHTI-hankkeen tuottamia ohjeita, joiden avulla julkishallinnon toimijat voivat kehittää tietoturvallisuuttaan. Ohjeet ovat päteviä myös yksityisellä sektorilla, jos yrityksessä halutaan käyttää tiedon luokittelutasoja. [Laaksonen ym. 2006: 30.]

4 Tietoturvallisuuden osa-alueet

Tietoturvallisuus voidaan jakaa osa-alueisiin. Osa-alueisiin jakaminen mahdollistaa tietoturvatoimenpiteiden suunnittelun, toteuttamisen ja valvonnan kokonaisvaltaisesti organisaatiossa. Tunnistetut riskit ja toteutettavat tietoturvatoimenpiteet voidaan jaottelun avulla kohdistaa tiettyyn osa-alueeseen.

Tietoturvallisuuden osa-aluejaottelua käytetään useissa standardeissa ja ohjeissa. Jaottelussa on usein pieniä eroja ja organisaation tulisikin valita, mitä jaottelua käytetään. Tässä työssä käytettäväksi jaotteluksi valittiin valtionhallinnon VAHTI-ohjeiden mukainen jaottelu ohjeiden kattavuuden, helpon saatavuuden ja toimeksiantajan organisaatioon soveltuvuuden takia. VAHTI-ohjeista eroavaa jaottelua käytetään esimerkiksi kansainvälisen standardisoimisjärjestön ISO 27000-standardiperheessä ja puolustusministeriön kansallisessa turvallisuusauditointikriteeristössä (KATAKRI).

4.1 Hallinnollinen turvallisuus

Hallinnollinen turvallisuus (engl. administrative controls) koostuu hyväksytyistä käytännöistä, toimintatavoista, standardeista ja ohjeista. Näillä voidaan ohjata organisaation ja sen työntekijöiden toimintaa sekä varmistamaan tietoturvan kehittäminen ja hallinta. [Information Security 2001.]

Hallinnolliseen turvallisuuteen kuuluvat esimerkiksi organisaation tietoturvatavoitteet, tietoturvapolitiikka, tietojärjestelmäkuvaukset, toimintaprosessit, riskianalyysi, tietoturvallisuuden organisointi ja vastuut sekä tietoturvallisuuden tavoitteiden saavuttamiseen käytettävät keinot. [Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004: 27-29.]

Organisaation johdon sitoutuminen tietoturvallisuuden kehittämiseen on tietoturvatyön perusta. Ylimmällä johdolla tulisi olla ymmärrys turvallisuuden perusvaatimuksista ja tieto järjestelmäkokonaisuuksista sekä niihin liittyvistä prosesseista ja riskeistä. Tietoturvallisuutta tulisi hallita kokonaisuutena, siten että koko organisaatiossa ymmärretään samat tavoitteet ja toimintatavat. Johdon näkemys tietoturvallisuuden tavoitteista ja tärkeydestä organisaatiosta ilmaistaan tietoturvastrategian ja -politiikan avulla. Asetet-

tujen tavoitteiden toteutumista tulee ohjata ja seurata. [Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004: 30-31.]

Hallinnollisen turvallisuuden menetelmiä käsitellään tarkemmin luvussa 5.

4.2 Henkilöstöturvallisuus

Henkilöstöturvallisuudella tarkoitetaan henkilöstöstä aiheutuvien tietoturvauhkien hallintaa. Henkilöstöturvallisuus koskettaa kaikkia organisaation työntekijöitä, ja sen toiminnassa haasteena on ihminen. Henkilöstöllä on keskeinen rooli tietojen käsittelyssä tiedon elinkaaren aikana, ja henkilöstöturvallisuustyön tavoitteena on ehkäistä tiedon käsittelyyn liittyviä uhkia. [Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta, VAHTI 2/2008: 11-12.]

Henkilöstöturvallisuuteen kuuluvat esimerkiksi rekrytoinnin aikana sekä työsuhteen alussa, lopussa ja sen aikana tehtävät toimenpiteet. Näitä ovat esimerkiksi soveltuvuuden tarkistaminen, riittävä perehdytys, sijaisuusjärjestelyt, tietoturvakoulutus, käyttöoikeuksien hallinta ja niiden poistaminen. Henkilöstöturvallisuuteen liittyvät myös työntekijän kanssa tehtävät sopimukset, esimerkiksi työsopimus ja salassapitosopimus. [Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004: 39-41.]

Henkilöstö saattaa toiminnallaan aiheuttaa tietojen eheyteen, luottamuksellisuuteen ja käytettävyyteen liittyviä uhkia joko tahallisesti tai tahattomasti. Myös organisaation rakenne ja menettelytavat saattavat aiheuttaa uhkia. Henkilöstöllä on suuri rooli tietoturvallisuuden tavoitteiden toteuttamisessa ja organisaation tulisi määriteltävät henkilöiden tietoturvallisuuteen liittyvät vastuut ja velvollisuudet esimerkiksi sopimusten ja tehtäväkuvausten avulla. Tahattomien vahinkojen hallinta voidaan toteuttaa muun muassa ohjeistamalla, kouluttamalla, kehittämällä työmenetelmiä ja vaikuttamalla asenteisiin. Tahallisia vahinkoja voidaan vähentää esimerkiksi tiedon luokittelulla, sisäisellä valvonnalla ja tarkastuksella, kulunhallinnalla sekä raportoinnilla. [Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta, VAHTI 2/2008: 19-20.]

4.3 Tietoaineistoturvallisuus

Tietoaineistoturvallisuuteen kuuluvat keinot asiakirjojen, tiedostojen ja muiden tietoaineistojen tietoturvallisuuden ylläpitämiseksi. Keinoilla pyritään suojaamaan tärkeiden tietoaineistojen eheys, luottamuksellisuus ja käytettävyys. Tietoaineistoturvallisuuden laiminlyönti voi aiheuttaa rikosoikeudellisen vastuun. [Laaksonen ym. 2006: 67.]

Tietoaineistoturvallisuuteen kuuluvat asiakirjan elinkaaren aikana tehtävät suojaavat toimenpiteet, esimerkiksi tiedon luokittelu, pääsynvalvonta, salassapito, käsittelysäännöt, käyttöoikeuksien määrittäminen, turvallinen säilyttäminen, asianmukainen arkistointi ja hävittäminen. Tiedolla tulisi olla omistaja, joka päättää tiedon luokituksesta, käytöstä ja jakelusta. Tietoaineistot tulisi säilyttää riittävän turvallisesti siten, että tiedon kriittisyys huomioidaan. Lisäksi tiedon suojaamisessa on huomioitava lain asettamat velvoitteet. [Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004: 79-84.]

Tietoaineistojen turvaamisessa tärkeää on tiedon luokittelun huomioiminen. Eri tavalla luokitellut tiedot tulee säilöä, käsitellä ja hävittää eri tavalla. Näin säästytään ylimääräisiltä kustannuksilta ja säilytetään salassa pidettävän tiedon luottamuksellisuus. Tietoaineistojen luokittelussa voidaan soveltaa julkisuuslain mukaista luokitteluasteikkoa, joka on tarkemmin eriteltynä taulukossa 1.

Taulukko 1. Tietoaineistojen luokittelu [Kansallinen turvallisuusauditointikriteeristö (KATAKRI) versio II 2009: 124.]

Suojaustaso	**Turvallisuusluokitus**	**Oikeudettoman paljastumisen tai käytön vaikutus**
Suojaustaso I	Erittäin salainen	Erityisen suurta vahinkoa yleiselle edulle
Suojaustaso II	Salainen	Merkittävää vahinkoa yleiselle edulle
Suojaustaso III	Luottamuksellinen	Vahinkoa yleiselle tai yksityiselle edulle
Suojaustaso IV	Käyttö rajoitettu	Haittaa yleiselle tai yksityiselle edulle, viranomaisen toimintaedellytysten heikkeneminen, rajoittava käyttötarkoitussidonnaisuus

Tietoaineistojen käsittelyn periaatteita tulisi soveltaa sekä paperiseen että sähköisessä muodossa käsiteltävään tietoon. Suojaustaso on hyvä merkitä asiakirjaan tai tietoaineistoon selkeästi, jotta tietoa käsittelevä taho tiedostaa käsittelevänsä luokiteltua tietoa.

4.4 Fyysinen turvallisuus

Fyysisellä turvallisuudella tarkoitetaan toimia, joilla hallitaan tiloihin, laitteisiin, henkilöstöön tai muihin organisaation resursseihin kohdistuvia fyysisiä uhkia. Näitä uhkia ovat esimerkiksi murto, varkaus, tulipalo, vesivahinko, sähköhäiriö ja pöly. Organisaatio tarvitsee fyysiset tilat toimiakseen, joten fyysinen turvallisuus luo pohjan kaikille muille tietoturvatoimenpiteille. [Laaksonen ym. 2006: 125-126; Physical Security 2015.]

Fyysiseen turvallisuuteen kuuluvat esimerkiksi toimitilojen tärkeysluokitus, kulunvalvonta, hälytysjärjestelmät, ilmastointi ja varavirtajärjestelmät. Toimitilojen tärkeysluokituksella voidaan tunnistaa tilojen tärkeys tietoturvan kannalta. Sen avulla voidaan asettaa sopivat turvatoimenpiteet kuhunkin tilaan, jolloin vältytään liiallisilta kustannuksilta ja virhearvioilta. Pääsy tietoturvan kannalta tärkeisiin tiloihin tulisi olla valvottu ja luvaton pääsy tulisi voida havaita. Tämä voidaan toteuttaa esimerkiksi hälytyslaitteistolla, joka ilmoittaa vartiointiliikkeelle tai vastaavalle taholle. Tietoturvan kannalta on tärkeää tietää, kenellä on pääsy tärkeisiin tiloihin. Kulkuoikeuksien ja fyysisten avainten jakelu on siis hoidettava hallitusti. [Laaksonen ym. 2006: 125-127.]

Toimitilojen luokittelussa voidaan soveltaa esimerkiksi valtionhallinnon toimitilojen turvallisuusvyöhykejakoa. Vyöhykejako perustuu tiloissa käsiteltävän ja säilytettävän tiedon suojaustasoon. Julkisuuslain mukaiset suojaustasot on eritelty tarkemmin taulukossa 1. Vyöhykejako on esitelty taulukossa 2. [Toimitilojen tietoturvaohje, VAHTI 2/2013: 21-22.]

Taulukko 2. Valtionhallinnon toimitilojen turvallisuusvyöhykejako

Turvallisuusvyöhyke (väritunnus)	**Suojaustaso**	**Käsiteltävä ja säilytettävä tietoaineisto**
Julkinen tila (VALKOINEN)	Ei suojaustasoa	Julkiset tietoaineistot, satunnaisesti suojaustason IV tietoaineistot
Perustason tila (VIHREÄ)	Suojaustaso IV	Suojaustason IV tietoaineistot
Korotetun tason tila (KELTAINEN)	Suojaustaso III	Suojaustason III tietoaineistot
Korkean tason tila (SININEN)	Suojaustaso II	Suojaustason II tietoaineistot
Erittäin korkean tason tila (PUNAINEN)	Suojaustaso I	Suojaustason I tietoaineistot

Vyöhykeluokittelu voi organisaatiosta riippuen seurata jotain muutakin luokittelutasoa, mutta se olisi hyvä liittää asiakirjojen luokittelutasoihin.

4.5 Laitteistoturvallisuus

Laitteistoturvallisuudella tarkoitetaan tietoturvallisuuden toteuttamiseksi tehtäviä toimia, jotka liittyvät tietojenkäsittely- ja tietoliikennelaitteiden ja tilojen käytettävyyteen, toimivuuteen, kokoonpanojen määrittelyyn ja pääsynvalvontaan sekä varaosien ja tarvikkeiden saatavuuteen. [Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004: 61.]

Laitteistoturvallisuuteen kuuluvat laitteiston elinkaarta turvaavat toimenpiteet esimerkiksi asennus, takuu, ylläpito, tukipalvelut sekä laitteiston poisto. Tietoturvan kannalta on tärkeää, että laitteistoon liittyvät palvelutasosopimukset tehdään asianmukaisesti. Tämä pätee erityisesti, jos koko palvelu tai osa organisaation laitteista sijaitsee palvelun tarjoajalla. Tämä aiheuttaa haasteita fyysisen turvallisuuden järjestelyille ja pääsynhallinnalle. Tällaisessa tapauksessa palvelutasosopimukseen tulisi sisällyttää kuvaukset verkkoyhteyksistä ja fyysisestä pääsystä järjestelmään poikkeamatilanteissa. [Tietoturvallisuudella tuloksia, VAHTI 3/2007: 63]

Laitteistoa voidaan hankkia varalle mahdollisia käyttökatkoja varten. Tarvittavaa varalaitekapasiteettia voidaan arvioida riskianalyysin ja laitteiden käyttökatkojen tilastoimisen avulla. Hankitut laitteet tulisi merkitä rekisteriin ja niiden toiminnan tilaa tulisi voida tarkkailla. Asennusvaiheessa laitteisto pitäisi tarkastaa, että se vastaa tilattua ja toimitettua laitetta. Laitteiston käytön aikana tapahtuviin mahdollisiin katkoihin on varaudut-

tava ennakoivasti järjestelmille asetettujen tietoturvatasojen mukaisesti. Laitteiston käytöstä poisto on suunniteltava ennalta. Poistomenetelmissä tulisi ottaa huomioon laitteiston sisältämän datan poisto tietoturvatason vaatimin toimenpitein. [Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004: 62-64.]

4.6 Ohjelmistoturvallisuus

Ohjelmistoturvallisuudella tarkoitetaan tietoturvallisuuden toteuttamiseksi tehtäviä toimenpiteitä, jotka kohdistuvat käyttöjärjestelmiin ja muihin ohjelmiin tai sovelluksiin. Näillä tarkoitetaan esimerkiksi tunnistamis- ja suojausominaisuuksia, valvonta- ja lokimenettelyjä sekä ylläpitoon ja päivitykseen liittyviä asioita. [Tietoturvallisuudella tuloksia, VAHTI 3/2007: 69.]

Ohjelmistoturvallisuuteen kuuluvat ohjelmiston elinkaaren aikana suoritettavat toimenpiteet, kuten dokumentointi, asennus, lisenssien hallinta, ylläpito ja tuki, tiedon varmistaminen, haittaohjelmien torjunta sekä käyttäjien koulutus. Ohjelmistojen asennuksessa on huomioitava rajapintojen ja laitteiston tietoturvavaatimukset. Näistä korkein määrittää sovellettavan tietoturvavaatimuksen ohjelmistolle. Ohjelmistoissa tulisi olla käytön aikana mahdollisuus tarkkailla käyttöä ja käyttöä sekä havaita väärinkäytöstapauksia. Tämä voidaan toteuttaa loki- ja raportointitoimintoja käyttämällä. Lokien ja raporttien hallinnassa on huomioitava yksityisyyden suojan velvoitteet. [Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004: 67-69, 74, 77.]

4.7 Tietoliikenneturvallisuus

Tietoliikenneturvallisuudella tarkoitetaan tietoturvallisuuden toteuttamiseksi tehtäviä toimia, jotka liittyvät tietoverkoissa kulkevaan tietoon, niitä ovat esimerkiksi laitteistojen ylläpito, verkonhallinta, pääsynvalvonta, tietoliikenteen käytön valvonta, ongelmatilanteiden hallinta ja viestinnän salaus. [Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004: 54.]

Tietoliikenneturvallisuuteen kuuluvat muun muassa tietoverkkojen eristäminen eri turvatasoilla, tietoliikenteen ajantasainen dokumentointi, tietoliikennelaitteiden ja kaapeloinnin suojaus, tunkeutumisen havaitsemis- ja estämisjärjestelmät, etäkäytön suojaa-

minen ja IP-puheluiden turvaaminen. [Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004: 54-55.]

Tietoliikenneverkoissa turvallisuus tulisi ottaa huomioon jo suunnitteluvaiheessa, jotta vältytään ylimääräisiltä kustannuksilta. Käytön aikana tehdyt muutokset verkkoon ovat yleensä kalliimpia kuin etukäteen suunnitellut vastaavat ratkaisut. Suunnitteluvaiheessa olisi hyvä huomioida tietoverkon turvallisuustavoitteet, joiden pohjalta tietoverkon turva-arkkitehtuuri voidaan suunnitella. Tietoverkon turva-arkkitehtuuriin kuuluvat esimerkiksi turvakomponenttien sijoittelu, verkon siirtokapasiteetin ja verkon valvonnan suunnittelu. Verkon vikasietoisuus tulee suhteuttaa verkon kriittisyyteen. Erittäin tärkeillä tietoverkoilla on syytä olla tehokkaat varajärjestelyt, joiden toiminta pitää testata. Verkon sallittu käyttö pitäisi suunnitella esimerkiksi tietoliikennepolitiikalla ja mahdollistaa verkon käytön valvonta riittävin resurssein, jotta käyttö vastaa verkolle asetettuja sääntöjä. [Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004: 55-58.]

4.8 Käyttöturvallisuus

Käyttöturvallisuudella tarkoitetaan tietotekniikan käyttöön, käyttöympäristöön tietojenkäsittelyyn ja sen jatkuvuuteen sekä tuki-, ylläpito-, kehittämis- ja huoltotoimintoihin liittyviä keinoja tietoturvallisuuden parantamiseksi. [Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004: 86.]

Käyttöturvallisuuteen kuuluvat muun muassa toimivuuden valvonta, etäkäytön periaatteet, käyttöoikeuksien hallinta, käytön ja lokien valvonta, varmuuskopiointi sekä häiriöraportointi. Esimerkiksi tietojärjestelmien suojaaminen haittaohjelmilta on osa käyttöturvallisuutta. Erityisesti toimintojen ulkoistaminen aiheuttaa haasteita käyttöturvallisuudelle. Ulkoistamistapauksissa olisi tärkeää tuntea oma toimintaympäristö ja ulkoistettava palvelu mahdollisimman hyvin, jotta palveluntarjoajalle osataan esittää riittävät vaatimukset turvallisuuteen ja käytettävyyteen liittyen. [Tietoturvallisuudella tuloksia, VAHTI 3/2007: 65; Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004: 89.]

5 Tietoturvallisuuden johtaminen ja hallinta

Tietoturvallisuuden lähtökohtainen tarkoitus on turvata organisaation toiminnalle tärkeiden tietojen eheys, luottamuksellisuus ja käytettävyys. Tietotekniikasta on tullut tärkeä osa nykyaikaisen organisaation toiminnan tehokkuutta, ja monet organisaation toiminnot riippuvat tietotekniikan toiminnan laadusta. Teknisten järjestelmien toiminta tulisi varmistaa normaaliolojen lisäksi myös poikkeus- ja erityistilanteissa, jotta organisaation toiminta ei häiriinny. [Tietoturvallisuudella tuloksia, VAHTI 3/2007: 13.]

Tietoturvallisuuden kehittämien ja tehokas johtaminen vaatii organisaation johdolta riittävät resurssit. Organisaation tulisi liittää tietoturvallisuus osaksi jokapäiväistä toimintaa ja liittää se työntekijöiden rutiineihin. Tämä voidaan toteuttaa esimerkiksi työhön liittyvien ohjeiden, perehdytyksen ja työnohjauksen kautta. [Laaksonen ym. 2006: 20, 115-116.]

Tietoturvallisuuden hyvä johtaminen ja organisaation tietoturvakulttuurin kehittäminen mahdollistavat kustannustehokkaan riskienhallinnan ja sitä kautta toimivan tietoturvallisuuden hallintajärjestelmän. [Tietoturvallisuudella tuloksia, VAHTI 3/2007: 15.]

5.1 Tietoturvallisuuteen liittyvät standardit

Lainsäädännöllisen kehyksen asettamat velvollisuudet ja oikeudet toimivat lähtökohtana organisaation tietoturvallisuuden hallinnan suunnittelussa. Tietoturvallisuuden hallinta vaatii hallinnollisia toimenpiteitä, koska pelkillä teknisillä ratkaisuilla ei voida toteuttaa hallittua tietoturvallisuutta. Tietoturvallisuuden hallinnointiin on kehitetty useita standardeja, ohjeita ja toimintatapoja, joita voidaan soveltaa organisaatioissa. Organisaatio voi valita standardeista itselleen parhaiten sopivan mallin tai yhdistellä eri standardien parhaita puolia. [Laaksonen ym. 2006: 83.]

Standardien sisältöä ei käsitellä tarkemmin tässä insinöörityössä, koska hallintajärjestelmän suunnittelussa sovelletaan pääosin valtiovarainministeriön VAHTI-ohjeita.

Tietoturvallisuuteen ja sen hallinnointiin liittyviä standardeja ovat esimerkiksi [Laaksonen ym. 2006: 88, 92, 95, 100]:

- ISO 27000 -standardiperhe
- COBIT (Control Objectives for Information and related Technology)
- ITIL (Information Technology Infrastructure Library)
- GAISP (Generally Accepted Information Security Principles).

Standardeja ja tunnettuja toimintamalleja hyödyntämällä organisaation tietoturvallisuudesta vastaava taho voi olla suhteellisen varma, että tietoturvallisuuden oleellisimmat osa-alueet tulee huomioitua. Tunnettuja malleja käyttävän organisaation joutuessa oikeudelliseen vastuuseen tietoturvallisuuden pettäessä voidaan helpommin todentaa, että tietoturvallisuuteen liittyvät toimenpiteet on suoritettu riittävän huolellisesti. Riippumatta siitä, käyttääkö organisaatio jonkin tietyn standardin mukaista mallia vai kehittääkö se itse toimintamallinsa, lain asettamat velvoitteet on otettava huomioon ensisijaisina. Esimerkiksi verkon valvontaan liittyvät standardien suosittelemat työkalut eivät välttämättä ole lain mukaan sallittuja. [Laaksonen ym. 2006: 104-105.]

5.2 Tietoturvallisuuden organisointi

Johdon sitoutuminen tietoturvallisuuden kehittämiseen on perusedellytys toiminnalle asetettujen tavoitteiden saavuttamiseen. Tietoturvallisuuden johtaminen tulisi sisällyttää organisaation kokonaisturvallisuuteen siten, että tietoturvallisuudelle asetetut tavoitteet tukevat muiden strategioiden turvallisuustavoitteita. Tietoturvallisuuden organisointi tulisi toteuttaa siten, että raportointi tapahtuu suoraan johdolle ja että tietoturvavastuut sisällytetään johtamisjärjestelmään, johtosääntöihin, työjärjestyksiin ja toimenkuviin. Vastuumäärittelyjen tulisi seurata organisaatiossa tapahtuvia muutoksia. [Tietoturvallisuudella tuloksia, VAHTI 3/2007: 27-28.]

Selkeillä vastuumäärittelyillä saadaan aikaiseksi toimiva ja hallittu kokonaisuus. Koko henkilöstön sitouttaminen ja organisaation tietoturvakulttuurin kasvattaminen tehostavat toimintaa pitkällä tähtäimellä.

5.2.1 Ylin johto

Organisaation johdon sitoutuminen tietoturva-asioihin alkaa tietoturvapolitiikan käsittelystä. Johdon sitoutumisen tulisi näkyä koko henkilöstölle osallistumisena tietoturvalli-

suuden kehittämisessä. Henkilöstölle tulee tiedottaa tietoturva-asioista ja mahdollistaa henkilöstön osallistuminen asioiden valmisteluun. Johdon tulisi myös näyttää esimerkkiä henkilöstölle seuraamalla organisaation tietoturvaohjeita. Näin myös henkilöstö sitoutuu paremmin tietoturvallisuudelle asetettuihin tavoitteiden saavuttamiseen. Johdon tärkeimpiin tehtäviin kuuluu tietoturvapolitiikan käsitteleminen ja riittävien resurssien varaaminen tietoturvatyöhön. Tätä varten johdolla tulee olla näkemys organisaatiolle tärkeiden tietojen suojaustarpeesta, tietoriskeistä ja niiden hallinnasta sekä siihen liittyvän työn vaatimista resursseista. Johdon tulee myös ohjata tietoturvallisuuden kehittämistä oikeaan suuntaan. [Laaksonen ym. 2006: 129-130.]

5.2.2 Tietoturvaorganisaatio

Tietoturvaorganisaatioksi kutsutaan sitä ryhmää, joka koordinoi tietoturvapolitiikan ja toimintaohjeiden laatimisen sekä järjestää henkilöstölle tarvittavan koulutuksen.

Tietoturvaorganisaation tehtäviin kuuluu esimerkiksi [Laaksonen ym. 2006: 132.]:

- ohjerungon kehittäminen koko organisaatiolle ja eri toimintayksiköille
- teknisen suojauksen suunnittelu yhdessä teknisten asiantuntijoiden kanssa
- tietoturvallisuuden toteutumisen valvonta projekteissa
- tietoturvallisuuden huomioiminen sopimuksissa ja sopimuskumppaneille asetettujen velvoitteiden seuranta
- yksilöiden toiminnan valvominen
- tietoturvakeskustelun seuraaminen
- esimiesten kouluttaminen tietoturvallisuuden jalkauttamisesta.

Tietoturvaorganisaation jäsenet hoitavat usein tietoturvaan liittyviä tehtäviä muiden tehtäviensä ohessa. Tavallisesti pienissä yrityksissä tietoturvaorganisaatio koostuu vain yhdestä henkilöstä, jolla on riittävät valmiudet ja resurssit sekä aito kiinnostus tehtävään. Tietoturvaorganisaatioon voi kuulua esimerkiksi laatujärjestelmistä vastaavat henkilöt, organisaation lakimies, tietohallinnon edustaja ja keskeisten prosessien omistajat. [Laaksonen ym. 131.]

5.2.3 Tietohallinto

Tietohallinto vastaa tietoturvallisuuden teknisestä toteuttamisesta tiedon, prosessien ja järjestelmien omistajien määrittämän suojaustason mukaisesti. Yleensä nämä tahot eivät kuulu tietohallintoon. [Laaksonen ym. 2006: 135.]

Tietohallinnon tehtäviin kuuluu muun muassa [Laaksonen ym. 2006: 136.]:

- teknisten tietoturvatoimenpiteiden toteuttaminen, dokumentointi ja suunnittelu yhdessä tietoturvasta vastaavien tahojen ja prosessin, tiedon ja järjestelmien omistajien kanssa
- loogisten pääsykontrollien hallinta yhdessä pääkäyttäjän kanssa
- käyttöoikeusmenettelytapojen noudattaminen
- tietojärjestelmien varmistaminen ja tiedonsiirron turvaaminen
- lokitietojen kerääminen ja säilyttäminen
- muutosten testaaminen ennen käyttöönottoa.

Tietojärjestelmien muodostamien lokien analysoiminen ei välttämättä kuulu tietohallinnolle. Tätä tehtävää ei kannata asettaa tietojärjestelmän pääkäyttäjän vastuuksi. Lokitietojen analysoinnin perusteella voidaan raportoida johdolle organisaation tilasta. Lokitietojen käsittelyssä tulee aina ottaa huomioon tunnistamistietojen käsittelyyn liittyvät määräykset. Tietohallinto vastaa joskus kiinteistöhuollon sijaan myös laitetilojen suojaamisesta, kulunvalvonnasta ja monitoroinnista. [Laaksonen ym. 2006: 135-136.]

5.2.4 Järjestelmien pääkäyttäjät

Tietoturvallisuuden hallinnan kannalta on tärkeää, että jokaiselle järjestelmälle on nimetty pääkäyttäjä, joka siitä että järjestelmä toimii oikein ja että sen prosessoima tieto on luotettavaa. Pääkäyttäjä vastaa yleensä järjestelmän käyttöoikeuksien hallinnasta, mutta ei päätä niistä. Prosessin, tiedon tai järjestelmän omistajan tulee päättää siitä, kenelle käyttöoikeudet annetaan.

Järjestelmän pääkäyttäjän tehtäviin kuuluu [Laaksonen ym. 2006: 135]:

- käyttöoikeuksien hallinta järjestelmään saatujen ohjeiden mukaisesti

- tietojen varmistaminen ja säilytys yhdessä tietohallinnon kanssa
- järjestelmän päivittäminen ja ylläpito muutoshallinnon prosessien mukaisesti
- käyttäjien tunteminen
- järjestelmän käytön seuranta.

Yleensä pääkäyttäjä nimetään sovelluksen käyttäjien joukosta. Pääkäyttäjän rinnalle voidaan nimetä tekninen pääkäyttäjä, joka voi tukea käytettyä järjestelmää sekä sen vaatimia käyttöjärjestelmiä ja laitteita. [Laaksonen ym. 135.]

5.2.5 Työntekijät

Organisaation työntekijöiden tulisi omalta osaltaan huolehtia tietoturvapolitiikan ja toimintaohjeiden noudattamisesta sekä osallistuttava koulutuksiin ja kyettävä soveltamaan saamiaan ohjeita työtehtävissään. [Laaksonen ym. 2006: 137.]

Jokaisen työntekijän tehtäviin kuuluu [Laaksonen ym. 2006: 137]:

- tiedon luokittelu ja käsittely sekä luokitellun tiedon käsittely, siirtäminen ja säilyttäminen ohjeiden mukaisesti
- omien salasanojen hallinta ja turvallinen käyttö
- ohjeiden noudattaminen
- varahenkilön tiedottaminen ja koulutus
- raportointi sovittuja raportointikanavia käyttäen.

Työntekijän tulee toimia työsopimuksen ja muiden tehtyjen sopimusten mukaisella tavalla. Tärkeässä asemassa olevan työntekijän tulisi pitää huolta myös varahenkilön tietojen ajantasaisuudesta. [Laaksonen ym. 2006: 137.]

5.2.6 Tietojen omistajat

Tiedon omistaja voi olla henkilö, joka tuottaa tai luo tiedon, tai prosessiin liittyvissä tiedoissa kyseisen toiminta-alueen johtaja. Tiedon omistaja päättää tiedon luokittelun ja

sen, kenellä on pääsy tietoon. Organisaation tulisi miettiä jokin tapa, jolla kaikelle tiedolle ja järjestelmille nimetään omistaja. [Laaksonen ym. 2006: 132-133.]

Tiedon omistajan tehtäviin kuuluu [Laaksonen ym. 2006: 133]:

- tiedon luokittelusta ja suojaustarpeesta sekä riittävästä tietoturvallisuuden tasosta päättäminen
- käyttäjien koulutus tiedon käsittelyn osalta
- tiedon käyttöoikeuksista päättäminen
- käyttöoikeuksien läpikäynti järjestelmän pääkäyttäjän kanssa
- tiedon suojaustason varmistaminen.

Organisaation henkilöstön toimintaohjeet tulisi muotoilla siten, että tiedon omistajan määrittämä tiedon luokittelu huomioidaan. Lain vaatimukset tiedon käsittelijän suhteen tulee ottaa huomion siten, että käsittely on lainmukaista. Lähtökohtaisesti kuka tahansa ei saa käsitellä tietoa, vaan käsittelyn on kuuluttava tiedon käsittelijän työtehtäviin. [Laaksonen ym. 2006: 133.]

5.2.7 Prosessien omistajat

Prosessiajattelumallia käytettäessä kullekin prosessille tulisi nimetä omistaja, jolla on operatiivinen vastuu kyseisestä prosessista [Laaksonen ym. 2006: 134].

Prosessin omistajan tehtäviin kuuluu [Laaksonen ym. 2006: 134]:

- riskikartoituksesta vastaaminen
- prosessin tietoturvatasosta päättäminen ja suojaustason varmistaminen
- suojattavien kohteiden luokitteleminen
- jatkuvuussuunnitelmien laatiminen ja testaaminen yhdessä tietoturvaorganisaation ja tietohallinnon kanssa
- prosessissa käytettävien tietojenkäsittelytapojen tunteminen
- tietoturvallisuuden tavoitteiden yhdistäminen organisaation toiminnan tavoitteisiin.

- tietoturvallisuuden kehittämistoimenpiteiden yhdistäminen prosessin muuhun kehittämiseen
- henkilöstön osaamisen varmistaminen
- raportointi ja seuranta normaalioloissa ja poikkeustilanteissa.

Prosessin omistaja ei välttämättä itse tee kaikkia tehtäviään, vaan on vastuussa siitä, että ne toteutetaan. Prosessin omistajuuden haasteena on tiedon liikkuvuus organisaation eri osien välillä. Tiedon liikkuessa selkeiden vastuiden määrittely voi olla hankalaa.

5.2.8 Sisäinen ja ulkoinen tarkastus

Sisäinen valvontajärjestelmä on osa organisaation johtamisjärjestelmää. Sisäisen tarkastuksen avulla voidaan valvoa esimerkiksi tietoturvapolitiikan, toimintaohjeiden ja tietoturvaratkaisujen toteutumista ja laatua organisaatiossa. Sisäinen tarkastus soveltuu tähän tehtävään, koska riippumattomana tahona se ei ole ollut mukana laatimassa esimerkiksi tietoturvaohjeita. [Laaksonen ym. 2006: 136.]

Sisäisen tarkastuksen tehtäviin kuuluu [Laaksonen ym. 2006: 136]:

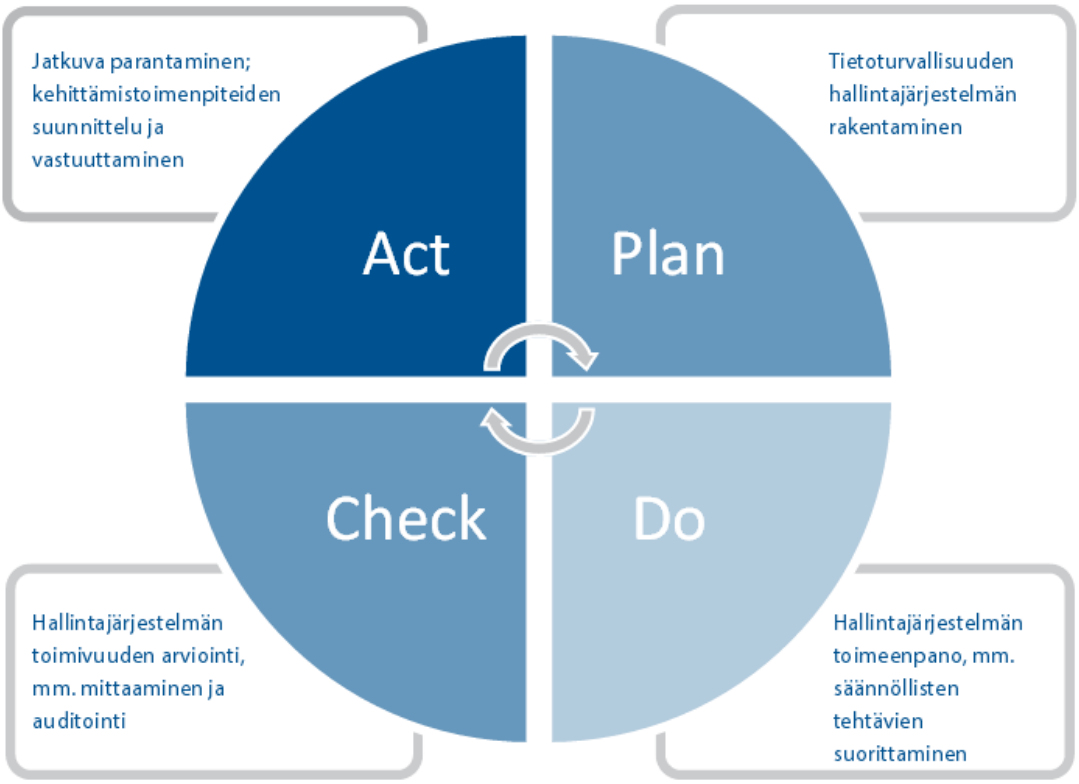
- tietojenkäsittelyn oikeellisuuden ja kontrolliympäristön toimivuuden arviointi
- raportointi organisaation johdolle
- kehitysehdotusten ja toimenpidesuositusten laatiminen.

Ulkoisella tarkastuksella tarkoitetaan käytännössä tilintarkastusta, jossa tarkastetaan tilinpäätös, kirjanpito ja yhtiön hallinto. Joskus tarkastetaan myös tietoturvaan liittyviä niiltä osin kun ne liittyvät tilinpäätöksen oikeellisuuteen. [Laaksonen ym. 2006: 137.]

5.3 Tietoturvallisuuden hallintajärjestelmä

Tietoturvallisuuden hallintajärjestelmällä tarkoitetaan johtamisjärjestelmän osaa, joka perustuu riskien arviointiin ja hallintaan. Sen tarkoituksena on suunnitella, toteuttaa, seurata, noudattaa, arvioida, ylläpitää ja kehittää tietoturvallisuutta. Hallintajärjestelmän toimivuus vaatii tietoturvallisuuden määrämuotoistamisen ja dokumentoinnin. [Laaksonen ym. 2006: 105-106.]

Tietoturvallisuuden hallintajärjestelmän jatkuvaan kehittämiseen käytetään usein PDCA-mallia (Plan, Do, Check, Act). PDCA on syklinen malli, joka perustuu jatkuvaan parantamiseen suunnittelun, tekemisen, arvioinnin ja parantamisen vaiheiden kautta. Tietoturvallisuuden PDCA-malli on tarkemmin kuvattuna kuvassa 1. Hallintajärjestelmää käyttävä organisaatio voi käyttää jotain muutakin vastaavaa mallia. Pääasia on, että organisaatio voi sen avulla kehittää hallintajärjestlemäänsä. [Information Security Management System 2004; Tietoturvallisuuden arviointiohje, VAHTI 2/2014: 14.]



Kuva 1. Tietoturvallisuuden PDCA-malli [Tietoturvallisuuden arviointiohje, VAHTI 2/2014: 15].

PDCA-mallia käytettäessä ei ole tarpeen, että yritetään suunnitella ensimmäisellä kerralla täydellinen järjestelmä, vaan pyritään tekemään siitä riittävän hyvä. Suunnittelun yhteydessä on hyvä arvioida käytössä olevat resurssit, että hallintajärjestelmä voidaan siirtää toimeenpanovaiheeseen ajallaan.

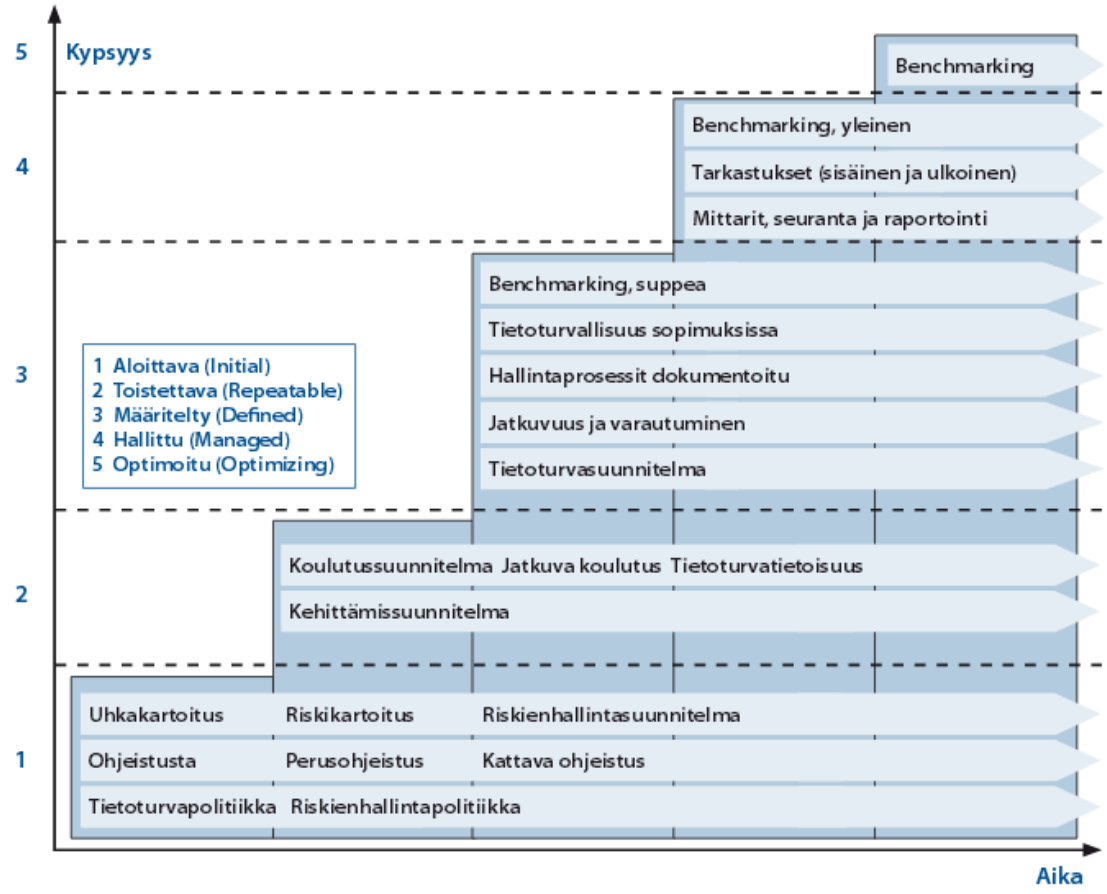
Hallintajärjestelmä on käytännössä kokoelma dokumentteja, jotka kuvaavat hallintajärjestelmän rungon. Hallintajärjestelmän ohjaamana tietoturvatyö on säännöllisempää, hallitumpaa ja luotettavampaa.

Tietoturvallisuuden hallintajärjestelmään liittyvien dokumenttien aiheita ovat esimerkiksi [Tietoturvallisuuden arviointiohje, VAHTI 2/2014: 15]:

- tietoturvapolitiikka ja -strategia
- tietoturvakäytännöt, -periaatteet ja -ohjeet
- kehittämissuunnitelma
- tietoturva-arkkitehtuurit
- riskienhallinnan kuvaus
- jatkuvuus- ja valmiussuunnitelmat
- tietoturvaraportointi
- auditointisuunnitelma.

Hallintajärjestelmän suunnittelussa tulee ottaa huomioon organisaatiota koskeva lainsäädäntö ja sopimukset, käytettävät standardit ja hallintajärjestelmän laajuus. Suunnitteluvaiheessa ei pyritä täydellisyyteen, sillä täydellistä järjestelmää ei voi luoda, vaan pyritään tekemään järjestelmästä riittävän laaja, että se voidaan ottaa käyttöön ja jalkauttaa organisaatioon.

Hallintajärjestelmän kehittämisessä voidaan hyödyntää kypsyysmalleja, joiden kautta voidaan määritellä tietoturvatoiminnan nykytila ja määrittelemään kehittämisen tavoitetaso, joka täyttää organisaation tietoturvallisuudelle asetetut vaatimukset. Erään valtionhallinnon organisaation näkemys tietoturvallisuuden kypsyystasoista on nähtävissä kuvassa 2. [Tietoturvallisuudella tuloksia, VAHTI 3/2007: 43.]



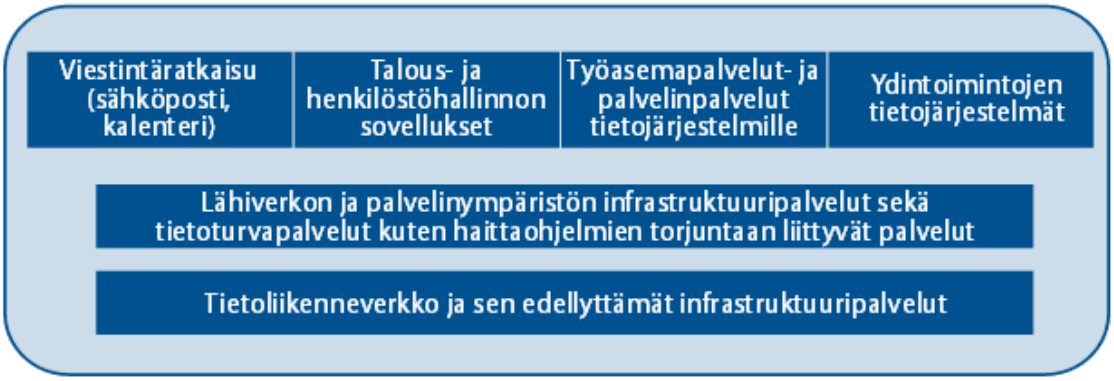
Kuva 2. Esimerkki kypsyysajattelun soveltamisesta [Tietoturvallisuudella tuloksia, VAHTI 3/2007: 42].

Tavoitellun tietoturvatason saavuttaminen vie yleensä useita vuosia. Tietoturvan kehittämisen tavoitteet voidaan liittää organisaation talous- ja toimintasuunnitelmiin ja jakaa useammalle vuodelle. Kehityksen mittaamiseksi sille pitäisi asettaa mitattavat vuositavoitteet. [Tietoturvallisuudella tuloksia, VAHTI 3/2007: 43.]

5.4 Suojattavien kohteiden tunnistaminen

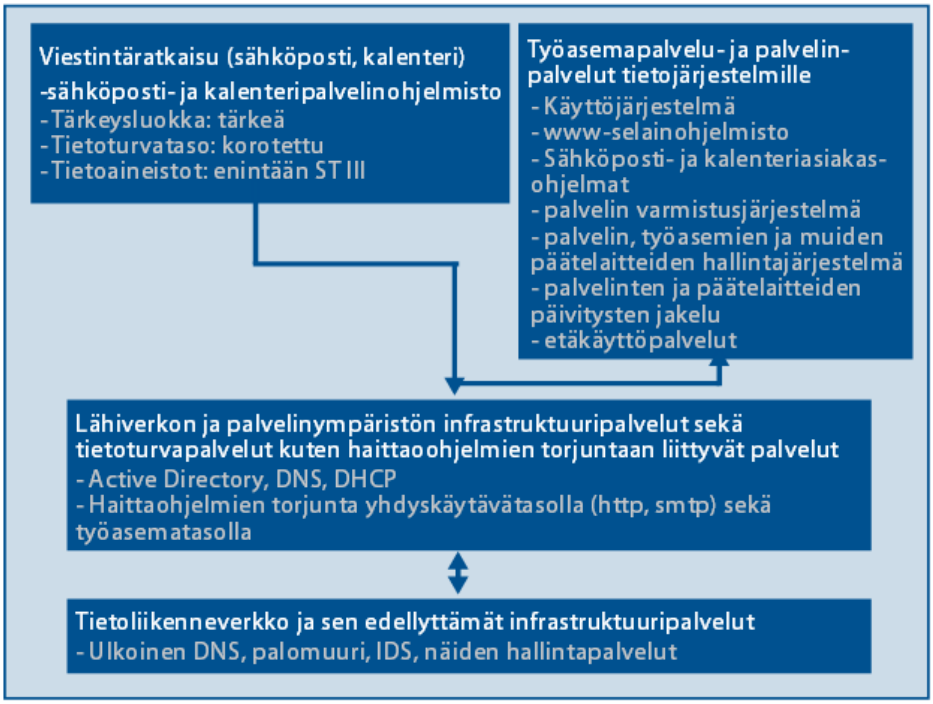
Suojattavalla kohteella tarkoitetaan organisaation toiminnalle tärkeää kokonaisuutta, joka luokitellaan jollekin tietoturvatasolle. Kohde voi olla esimerkiksi tietojärjestelmä, dokumentti, prosessi, fyysinen tila tai työasema. Suojattavien kohteiden määrittämistä varten on selvitettävä organisaatiota koskeva lainsäädäntö, määräykset, sopimukset, toimintaperiaatteet ja käytössä olevan teknologian rajoitukset ja vaatimukset. [Teknisen ICT-ympäristön tietoturvataso-ohje, VAHTI 3/2012: 31-32.]

Organisaation tulee tunnistaa sille kriittiset toiminnot ja prosessit sekä niitä tukevat tietojärjestelmät ja palvelut. Jotta kohde voidaan suojata asiallisesti, organisaation on luokiteltava käyttämänsä järjestelmät tärkeyden mukaan. Tärkeysluokituksessa määritellään myös haluttu tietoturvataso. Kuvassa 3 on esimerkki pienen organisaation käyttämistä ICT-palveluista kokonaisuutena. [Teknisen ICT-ympäristön tietoturvataso-ohje, VAHTI 3/2012: 33, 36.]



Kuva 3. Yksinkertaistettu kuva pienen organisaation käyttämistä ICT-palveluista [Teknisen ICT-ympäristön tietoturvataso-ohje, VAHTI 3/2012: 34].

Organisaation tulisi hahmottaa järjestelmien ja palveluiden muodostamat kokonaisuudet ja ymmärtää niissä käsiteltävän tiedon vaatimukset ja järjestelmän käytön tärkeys. Kokonaisuuden tarkastelu selkeyttää organisaation sisällä käsiteltävän tiedon liikkeitä ja mahdollisesti paljastaa epäkohtia. Luokiteltu tieto ja sille asetetut suojaustoimenpiteet saattavat aiheuttaa muutoksia myös luokiteltuun tiedon käsittelyyn läheisesti liittyvissä järjestelmissä. Esimerkki tästä on kuvassa 4, jossa kuvataan erään organisaation viestintäratkaisua.



Kuva 4. Organisaation viestintäratkaisun tietoturvallisuus [Teknisen ICT-ympäristön tietoturvataso-ohje, VAHTI 3/2012: 34].

Kuvasta voidaan havaita, että tietoaineiston tietoturvataso aiheuttaa sen, että myös muiden palveluiden tietoturvatasot tulee toteuttaa korotetulla tietoturvatasolla. Muutoin palvelun taso ei vastaa tietoaineiston vaatimaa suojaustasoa. Kun organisaatio on tunnistanut tärkeimmät kokonaisuudet, niihin liittyvät järjestelmät ja palvelut sekä kriittiset prosessit ja toiminnot, voidaan järjestelmät luokitella tärkeyden perusteella. Luokitteluun voidaan kehittää organisaation oma malli tai käyttää jotain sopivaa olemassa olevaa mallia.

VAHTI-ohjeissa järjestelmien tärkeysluokittelu perustuu seuraaviin tekijöihin [Teknisen ICT-ympäristön tietoturvataso-ohje, VAHTI 3/2012: 37]:

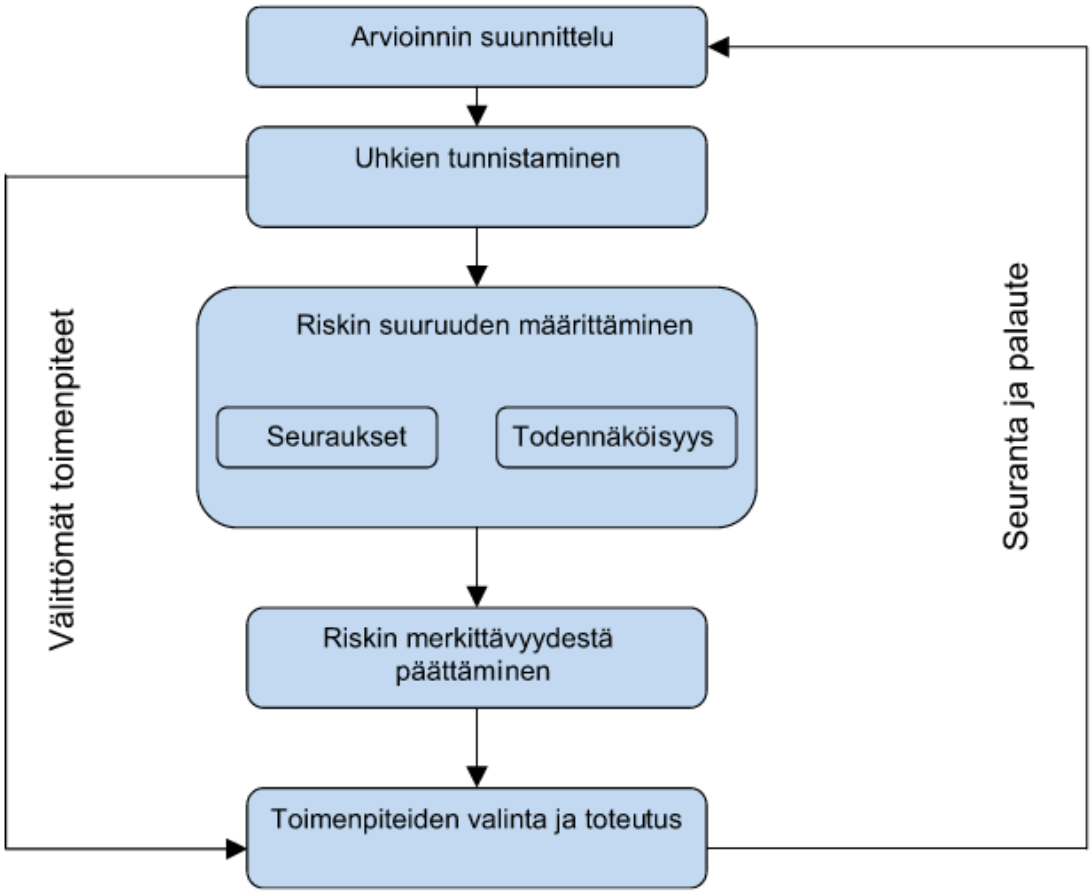
- asiakirjan luokittelu
- luottamuksellisuuden, eheyden ja käytettävyyden merkitys
- merkitys organisaation ydintoiminnoille
- merkitys asiakkaalle tai muulle toimintaverkostolle
- merkitys yhteiskunnalle.

Tärkeysluokittelun lisäksi on kannattavaa liittää suojattaviin kohteisiin vuosikello, jonka mukaan järjestetään ylläpito, johon voi kuulua esimerkiksi riskienhallinta, suunnitelmien päivitys, harjoittelu, katselmointi, raportointi ja muut toistuvat prosessit. [Teknisen ICT-ympäristön tietoturvataso-ohje, VAHTI 3/2012: 37.]

Tärkeysluokittelun perusteella voidaan priorisoida järjestelmiin kohdistettavia tietoturvatoimenpiteitä ja välttää ylimääräisiä kustannuksia tehokkaalla riskienhallinnalla.

5.5 Riskienhallinta

Riskienhallinnalla pyritään tunnistamaan ja hallitsemaan organisaation toimintaan haitallisesti vaikuttavia tapahtumia eli riskejä. Riskienhallinnan päävaiheet ovat uhkien tunnistaminen ja niiden merkityksen arviointi. Sen jälkeen suunnitellaan riskien torjumiseksi tarvittavat toimenpiteet. Kolmannessa vaiheessa suunnitellaan toimintaa uhkan toteutuessa ja miten vahingoista toivutaan. Tämän jälkeen tilannetta seurataan, toteutunut riski analysoidaan ja toimintaa kehitetään sen mukaisesti. Riskien arvioinnin ja hallinnan vaiheet on kuvattu pääpiirteittäin kuvassa 5. [Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003: 15.]



Kuva 5. Riskien arvioinnin ja hallinnan vaiheet [Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003: 16.]

Riskien arvioinnissa käytetään järjestelmällisiä toimenpiteitä, joiden avulla tunnistetaan tietoturvallisuuden uhkia ja haavoittuvuuksia sekä arvioidaan toteutuvien uhkien seurauksia. Toimenpiteet voivat vastata organisaation muuhun riskienhallintaan käytettäviä toimenpiteitä. Uhkien tunnistamiseen löytyy useita apuvälineitä, mutta lähtökohtaisesti tarvitaan kriittinen ja ennakkoluuloton asenne. Riskien arviointi kannattaa suorittaa ryhmätyönä, johon kuuluu analysoitavan kohteen tuntevia henkilöitä. [Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003: 16-18.]

Kun uhkat on tunnistettu ja riskien todennäköisyys ja vakavuus arvioitu päätetään toimenpiteistä riskin hallitsemiseksi.

Riskienhallinnan keinoja ovat [Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003: 21]:

- riskin välttäminen (vain jos toiminnasta luovutaan kokonaan)
- riskin poistaminen (poistaminen voi aiheuttaa muita riskejä)
- riskin pienentäminen (vähennetään seurausten vakavuutta tai tapahtuman todennäköisyyttä)
- riskin siirtäminen (sopimukset, vakuutukset)
- riskin pitäminen omalla vastuulla (tietoinen riski, että uhka voi toteutua).

Riskien pienentämiseksi voidaan suorittaa esimerkiksi teknisiä, organisaation toimintaa tai yksilöiden toimintamahdollisuuksia parantavia toimenpiteitä. Nämä vaativat resurssien käyttöä esimerkiksi uusien laiteratkaisujen, toimintaohjeiden laatimisen tai uusien työvälineiden hankinnan takia. Kustannukset on otettava huomioon, ennen kuin varsinaisia toimenpiteitä lähdetään toteuttamaan. Riskienhallinnalla ei pyritä poistamaan kaikkia riskejä, koska se on mahdotonta, vaan pyritään keskittymään vakavimpiin riskeihin niin laajasti kuin mahdollista. [Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003: 21-22.]

Uhkien tunnistamismenetelmistä ja muista riskienhallintaan liittyvistä vaiheista on tarkemmin eritelty VAHTI-ohjeissa. Riskienhallintaan liittyy myös kansainvälinen standardi ISO 17799 ja monet muut laajalle levinneet toimintamallit.

5.6 Tietoturvaohjeistus

Tietoturvallisuuden hallinnan tärkeimpiä osia on organisaation kaikki toiminnot kattava politiikka ja ohjeistus. Ohjeistus koostuu yleensä yksittäiseen tarkoitukseen laadituista ohjeista, jotka vastaavat jonkin standardin tai viitekehyksen vaatimuksia, kun taas tietoturvapolitiikassa käsitellään asioita yleisellä tasolla ja luodaan vaatimuksia joihin ohjeissa voidaan viitata. [Laaksonen ym. 2006: 145.]

Tietoturvapolitiikka on johdon kannanotto tietoturvalinjauksista organisaatiossa. Politiikan avulla osoitetaan johdon sitoutuminen tietoturvallisuuden kehittämiseen ja se luo perustan muulle tietoturvaohjeistukselle ja tietoturvan kehittämiselle. [Laaksonen ym. 2006: 146-147.]

Tietoturvapolitiikkaan sisältyy yleensä seuraavat asiat [Laaksonen ym. 2006. 147]:

- tietoturvallisuuden tavoitteet ja niihin liittyvä toiminta: miten tietoturvallisuus vaikuttaa organisaation toimintaan ja miten tietoturva-asioihin tulee suhtautua
- tietoturvallisuuden roolit ja vastuut: nimetään tahot, jotka vastaavat tavoitteiden saavuttamisesta
- tietoturvakoulutuksen vaatimukset tavoitteiden saavuttamisen kannalta
- tietojenkäsittelyn suojauksen suuntaviivat, esimerkiksi tietosisällön luokittelun käyttö
- yleiset linjaukset jatkuvuus- ja toipumissuunnittelun toteuttamisesta
- seuraukset tietoturvapolitiikan laiminlyönnistä.

Johdon tulee ymmärtää tietoturvapolitiikan sisältö. Politiikka voidaankin luoda siten, että johto keskustelee mainituista asioista ja laatii keskustelun pohjalta dokumentin. Johdon sitoutuminen valmiin mallin mukaiseen politiikkaan on heikompi, kuin jos johto käsittelee dokumentin hyvin. Tietoturvapolitiikka kannattaa tehdä mahdollisimman yleisellä tasolla siten, että jokainen lukija ymmärtää lukemansa. Se tulee myös pitää mahdollisimman lyhyenä, eikä siinä pidä puuttua tarkkoihin suojausmenetelmiin. Politiikan olisi hyvä olla myös jaettavissa ulkopuolisille tahoille, esimerkiksi asiakkaille, yhteistyökumppaneille tai muille tahoille joilla on pääsy organisaation tietojärjestelmiin. [Laaksonen ym. 2006: 148.]

Toimintaohjeistuksella pyritään siihen, että henkilöstö kykenee soveltamaan yrityksen tietoturvakäytäntöjä. Ohjeita tulisi laatia tarpeen mukaisesti ja jakaa niille henkilöille, jotka tarvitsevat ohjetta työssään. Ohjeiden laatiminen ei vielä yksinään riitä, vaan on myös varmistuttava, että ohje ymmärretään ja sen mukaan toimitaan. Ohjeistuksessa on painotettava henkilöstön tärkeää roolia ja heidän käsittelemänsä tiedon on tärkeyttä organisaatiolle. [Laaksonen ym. 2006: 161.]

Toimintaohjeet saattavat työntekijän mielestä muutosvastarinnan takia vaikuttaa aluksi ylimääräisiltä hidasteilta. Hyvän ohjeistuksen tekemiseksi on ymmärrettävä ohjeistettavien henkilöiden työnkuva. Tällä tavalla ohjeistus voidaan saattaa riittävän yksinkertaiseen ja ymmärrettävään muotoon, että se voidaan helposti yhdistää päivittäisiin työtehtäviin.

6 Tietoturvallisuuden hallinta seurakunnassa

Tietoturvallisuuden hallintajärjestelmän suunnittelun tarkoituksena oli luoda seurakunnalle keinot tietoturvan hallintaan, kehittämiseen ja ylläpitoon. Tarve hallintajärjestelmälle havaittiin, kun seurakunnan tietoturvallisuuteen kohdistuvia riskejä arvioitiin ulkopuolisen konsultin avulla. Selkeitä vastuita ei ole määritelty, eikä tietoturvariskeihin varauduttu suunnitelmallisesti etukäteen.

Hallintajärjestelmän suunnitteluun varattiin osa tietohallinnon työajasta. Suunnittelu aloitettiin rajaamalla hallintajärjestelmään laajuus. Hallintajärjestelmän kehittämiseen liittyvät dokumentit rajattiin seuraavasti:

- suojattavien kohteiden määrittely (järjestelmäkuvaus)
- riskienhallinnan työkalut
- tietoturvapolitiikka ja -ohjeistus
- tietoturvatasojen luokittelut.

Toimeksiantajalla ei ollut käytössä selkeää tapaa arvioida suojattavien kohteiden tärkeyttä. Toimeksiantajalle suunniteltiin tietoturvatasojen luokitteluun käytettävät kriteerit, jotta riskienhallinnasta tulisi tehokkaampaa.

Suunnittelussa sovellettiin VAHTI-ohjeita ja KATAKRI-auditointikriteeristöä.

6.1 Järjestelmäkuvaukset

Järjestelmäkuvausten avulla mahdollistetaan tietoturvallisuuden järjestelmällinen hallinta. Kuvausten avulla selviää, mitkä kaikki järjestelmät organisaatiolla on käytössä ja voidaan asettaa järjestelmät tärkeysjärjestykseen.

Toimeksiantajalle suunnitellussa järjestelmäkuvauksessa pyritään vastaamaan seuraaviin kysymyksiin:

- Mikä on järjestelmän käyttötarkoitus?
- Kuinka tärkeä järjestelmä on organisaation toiminnan kannalta?

- Millaista tietoa järjestelmässä käsitellään? (esim. henkilötiedot)
- Missä järjestelmää käytetään ja missä järjestelmään liittyvät laitteet sijaitsevat?
- Kuka on järjestelmän pääkäyttäjä, ylläpitäjä ja tekninen pääkäyttäjä? Ketkä järjestelmää käyttävät?

Järjestelmäkuvausten avulla voidaan tehdä tehokkaampaa riskienhallintaa. Järjestelmien tärkeysluokittelu mahdollistaa sen, että järjestelmälle asetetut tietoturvavaatimukset eivät ole liiallisia eikä niihin sitä kautta kulu ylimääräisiä kustannuksia.

Järjestelmien luokittelua ja suojattavien kohteiden määrittelyä on käsitelty aiemmin luvussa 5.

6.2 Riskienhallinta

Riskienhallintaa varten toimeksiantajalle suunniteltiin riskien kriittisyyden arviointiin käytettävä työkalu, jossa määritellään riskien vakavuus todennäköisyyden ja seurauksien vakavuuden perusteella. Näillä perusteilla riskit luokitellaan kriittisyyden perusteella ja hallitaan sitä kautta tehokkaasti.

Riskien vakavuuden määrittteleviä tekijöitä ovat:

- Kuinka moni taho voi aiheuttaa riskin toteutumisen?
- Kuinka moniin toimintoihin riskin toteutuminen vaikuttaa ja kuinka pitkään vaikutus kestää?
- Liittyykö riskin toteutumiseen tiedotusvelvollisuutta?
- Mihin tahoihin riskin toteutuminen vaikuttaa?
- Kuinka kiinnostava riskiin liittyvä suojattava kohde on ja kuinka kattavat toimintaohjeistukset kohteen käyttöön on?

Korkeamman kriittisyysluokan riskeihin pyritään puuttumaan ensimmäisenä, ja luokittelu sisältää myös mitättömien riskien luokan, joiden todennäköisyys ja vaikutukset ovat vähäiset.

Riskienhallinnan menetelmiä ja sen kehittämiseen käytettäviä ohjeita on käsitelty aiemmin luvussa 5.

6.3 Tietoturvaohjeistus

Toimeksiantajan toimintaohjeistuksessa ei ollut kunnolla huomioitu tietoturvaa. Tietoturvaohjeistus oli lähinnä suullisesti annettua, eikä se seurannut mitään selkeää linjaa. Tietoturvaohjeistuksen tekeminen aloitettiin laatimalla seurakunnalle tietoturvapolitiikka.

Tietoturvapolitiikan tarkoituksena on määrittää seuraavat asiat:

- johdon kannanotto tietoturvaan liittyviin asioihin
- tietoturvallisuuden toteutuskeinot
- tietoturvallisuuden organisointi ja vastuut
- tietoturvallisuudesta tiedottaminen (julkinen ja sisäinen)
- seuranta ja ongelmatilanteiden käsittely.

Tietoturvapolitiikka laadittiin siten, että pienet muutokset organisaation rakenteessa eivät vaadi välttämättä muutoksia tietoturvapolitiikkaan. Politiikasta tehtiin myös riittävän yleistasoinen, että sen voi mahdollisesti luokitella julkiseksi. Se on myös riittävän lyhyt ja yleisluonteinen, että se on helppo ymmärtää ja lukea läpi.

Tietoturvapolitiikan ja toimintaohjeiden kehittämistä on käsitelty aiemmin luvussa 5.

7 Yhteenveto

Insinöörityössä selvitettiin tietoturvallisuuden hallinnan menetelmiä ja edellytyksiä. Työn tarkoituksena oli kehittää toimeksiantajan tietoturvallisuuden hallinnan tilaa. Työ toteutettiin Helsingin ortodoksiselle seurakunnalle. Toimeksiannon taustalla oli halu kehittää tietoturvallisuuden hallintaa toimeksiantajan organisaatiossa. Erityisesti lainsäädännön asettamat vaatimukset haluttiin selvittää.

Työn aikana kerättiin tietoa tietoturvallisuutta koskevasta lainsäädännöstä, standardeista, hallintamalleista ja toimintaohjeista. Kerätyn tiedon perusteella kehitettiin tietoturvallisuuden hallintajärjestelmän runko. Työssä käytetyt lähteet antavat riittävän kuvan tietoturvallisuuden hallinnan ja johtamisen menetelmistä. Hallintajärjestelmän osat soveltuvat hyvin toimeksiantajan organisaation käyttöön.

Hallintajärjestelmän laajuus määriteltiin siten, että organisaatio voi ryhtyä sen avulla kehittämään tietoturvakulttuuriaan. Hallintajärjestelmää tulee jatkossa kehittää ja sen osia päivittää. Työssä kerätyt tietolähteet ja hallintajärjestelmän runko tekevät sen kuitenkin mahdolliseksi.

Lähteet

Asianhallinnan tietoturvallisuutta koskeva ohje, VAHTI 5/2006. 2006. Verkkodokumentti. Valtivarainministeriö. <https://www.vahtiohje.fi/c/document_library/get_file?uuid=4f7868bb-8f96-46f6-8b90-666928b4f32a&groupId=10128&groupId=10229>. Luettu 12.3.2015.

Henkilötietolaki (523/1999). 1999. Päivitetty 17.5.2011.

Information Security. 2001. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Information_security>. Luettu 20.4.2015.

Information Security Management System. 2015. Verkkodokumentti. Wikipedia. <http://en.wikipedia.org/wiki/Information_security_management_system>. Päivitetty 20.4.2015.

Kansallinen turvallisuusauditointikriteeristö (KATAKRI) versio II. 2009. Verkkodokumentti. Puolustusministeriö. <http://www.defmin.fi/files/1870/KATAKRI_versio_II.pdf>. Päivitetty 2011.

Laaksonen, Mika; Nevasalo, Terho & Tomula, Karri. 2006. Yrityksen tietoturvakäsikirja. Helsinki: Edita.

Laki viranomaisen toiminnan julkisuudesta (612/1999). 1999. Päivitetty 6.2.2015.

Laki yksityisyyden suojasta työelämässä (759/2004). 2004. Päivitetty 30.12.2014.

Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003. 2003. Verkkodokumentti. Valtiovarainministeriö. <https://www.vahtiohje.fi/c/document_library/get_file?uuid=d1bcc4b1-789e-4ce1-a44a-e591a60985b5&groupId=10128&groupId=10229>. Luettu 20.4.2015.

Rikoslaki (39/1889). 1889. Päivitetty 20.3.2015.

Rousku, Kimmo. 2014. Kyberturvaopas. Talentum.

Teknisen ICT-ympäristön tietoturvataso-ohje VAHTI 3/2012. 2012. Verkkodokumentti. Valtiovarainministeriö. <https://www.vahtiohje.fi/c/document_library/get_file?uuid=5a273c6e-2935-4bbf-a4c6-f00e0f878db5&groupId=10128&groupId=10229>. Luettu 20.4.2015.

Tietoturva. 2004. Verkkodokumentti. Wikipedia. <http://fi.wikipedia.org/wiki/Tietoturva>. Päivitetty 11.2.2015.

Tietoturvallisuudella tuloksia, VAHTI 3/2007. 2007. Verkkodokumentti. Valtiovarainministeriö. <https://www.vahtiohje.fi/c/document_library/get_file?uuid=8c85fe8f-aa4c-4e67-9236-2fee696498a9&groupId=10128&groupId=10229>. Luettu 26.2.2015.

Tietoturvallisuuden arviointiohje, VAHTI 2/2014. 2014. Verkkodokumentti. Valtiovarainministeriö. <https://www.vahtiohje.fi/c/document_library/get_file?uuid=ce1ccede-8669-4166-b084-9cafbe6e1e60&groupId=10128&groupId=10229>. Luettu 20.4.2015.

Tietoturvan peruskäsitteitä. 2012. Verkkodokumentti. Opetushallitus. <http://www.oph.fi/opetustoimen_turvallisuusopas/turvallisuuden_osa-alueita/tietoturva/tietoturvan_peruskasitteita>. Luettu 15.4.2015.

Tietoyhteiskuntakaari (917/2014). 2014. Päivitetty 19.12.2014.

Tietoyhteiskuntakaari. 2015. Verkkodokumentti. Liikenne- ja viestintäministeriö. <http://www.lvm.fi/web/hanke/tietoyhteiskuntakaari>. Luettu 9.4.2015.

Toimitilojen tietoturvaohje, VAHTI 2/2013. 2013. Verkkodokumentti. Valtiovarainministeriö. <https://www.vahtiohje.fi/c/document_library/get_file?uuid=78751ee8-c2c8-4ac4-945c-72cb9ec4a01b&groupId=10128&groupId=10229>. Luettu 20.4.2015.

Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta, VAHTI 2/2008. 2008. Verkkodokumentti. Valtiovarainministeriö. <https://www.vahtiohje.fi/c/document_library/get_file?uuid=af5614a4-fa44-482c-9886-0af9e6a13929&groupId=10128&groupId=10229>. Luettu 20.4.2015.

Valtionhallinnon keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004. 2004. Verkkodokumentti. Valtiovarainministeriö. <https://www.vahtiohje.fi/c/document_library/get_file?uuid=35e1f7af-9ecd-4787-8cbf-a685213cd4f8&groupId=10128>. Luettu 13.4.2015.